# Showcase Europe

# Guide to Internet Security Markets in Europe

*Your Global Business Partner*

# Table of Contents

# 1 European Union

## 1.1 Introduction

1. Internet security is a key element in the European Union's (EU) efforts to exploit the growth inducing, job creating potential of the digital economy. The 15 Member States agreed in the summer of 2000 on an initiative to get Europeans on-line – the **eEurope Action Plan[1].** Central to the plan is the objective of a cheaper, faster, and more secure Internet. EU member countries also committed themselves to promoting e-government, e-health, and e-procurement, all of which will drive the market for secure Internet access.

2. This report outlines the main initiatives flowing from eEurope and highlights other EU policy and regulatory developments that are likely to impact on the Internet security market. It covers EU legislation on electronic signatures and the free movement of encryption technology, as well as initiatives in the areas of cybercrime, smart cards and on-line payments. It also looks at the EU's regulatory framework for securing personal data, consumer rights and intellectual property in the on-line environment. All of these developments will contribute to shaping the market for security products and services.

3. In many cases the customers for Internet security solutions are the companies and organizations that must comply with these EU requirements – knowing your customers needs is half the battle. Decisions taken at EU level are either directly applicable or implemented in the Member States. For further information on any of the points raised in this report do not hesitate to contact the Commercial Service at the United States Mission to the European Union – Brussels.ec.office.box@mail.doc.gov

## 1.2 Cybercrime

4. Combating computer-related crime to create a safer Internet is one of the objectives of the eEurope Action Plan. The economic damage caused by disruptions such as virus and denial of service attacks is increasing. The European Commission argues that responsibility for ensuring awareness and take up of security products lies with industry but believes that the public sector, and itself in particular, can have a catalyzing role.

5. The Commission's **Communication on Cybercrime[2]**, adopted in January 2001, calls for an approximation of national laws in the area of high-tech crime and the setting up of an EU Forum to raise public awareness on the risks posed. The Forum will represent law enforcement agencies, service providers, network operators, consumer groups and data protection authorities, and aims to promote best practices for information technology security. Its work should be followed

[1] E-Europe http://www.europa.eu.int/comm/information_society/eeurope/index_en.htm.
[2] COM 2000/890 Communication on Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related crime http://europa.eu.int/ISPO/eif/InternetPoliciesSite/Crime/crime1.html

closely. Importantly, the Commission will assess the need for a legislative initiative on the issue of data retention on the basis of work conducted by the Forum.

6. EU **privacy laws for the telecoms sector**[3] state that data can only be kept for billing purposes and that it should be deleted or rendered anonymous once it is no longer needed for this commercial purpose. However some EU countries are requiring or allowing service providers to keep data where it could be useful for criminal investigation. This imposes a financial and administrative burden on service providers and risks distorting the Single Market.

7. The issue of interception creates similar problems. Under EU law there is a general principle of confidentiality of communications but national administrations can order interception according to strict rules. In the past this was simple to organize but now, faced with a plethora of service providers, some EU countries are introducing new technical interception requirements. Once again the integrity of the Single Market is threatened and, just as importantly, such initiatives clash with industry's attempts to roll out the technological solutions that will persuade consumers to consider the Internet as a sufficiently secure environment.

8. As more attention is given to the risks of the Internet's open network the market potential for security solutions will grow. Security lies with users and, as more of them carry out a broader range of activities on line, there will be more commercial opportunities in the Internet security market. What is important in the cybercrime debate is that the same encryption technologies that nurture user confidence can also be used to hide criminal activity.

### 1.3 Smart Cards

9. Smart Cards are singled out in the eEurope Action Plan as an effective means of addressing security concerns in a digital environment. The perception is that Europe has a solid smart card industry and that is only prevented from developing its full potential due to a lack of common standards and applications. The **eEurope Smart Card**[4] initiative has now triggered the setting up of twelve industry led working groups known as Trailblazers, which are working to establish specifications and guidelines on issues ranging from E-payments to security certification. The initiative is open to all organizations and businesses. Involvement provides an opportunity to be part of a process which is likely to set the parameters for security applications in the EU market.

10. The Commission is backing the Smart Card drive through the European Union's Fifth Framework Program for Research and Development, and in particular the **Information Society Technologies Program**[5]**.** The latest call for proposals in

---

[3] Directive 97/66 on the processing of personal data and the protection of privacy in the telecommunications sector http://europa.eu.int/eur-lex/en/lif/dat/1997/en_397L0066.html

[4] eEurope Smart Card Initiative www.cordis.lu/ist/ka2/smartcards.html

[5] EU FP 5 on Information Society Technologies http://www.cordis.lu/ist/home.html

February 2001 focuses on the development of multi-application Smart Cards. US companies established in the EU can participate in these programs and there are also opportunities for US based firms to participate through the US/EU Science and Technology Agreement. Involvement in these programs can lead to useful partnerships with European companies.

### 1.4 Electronic Signatures

11. The **Electronic Signatures Directive**[6] sets out a general framework that must be implemented by the Member States before 19 July 2001. The Directive aims to facilitate the use of electronic signatures and to contribute to their legal recognition. It defines requirements for certification services to ensure a guaranteed minimum level of security and to allow them to be delivered across the EU.

12. The Directive draws a distinction between advanced and regular electronic signatures. The advanced versions must be based on a qualified certificate and be created by a secure signature creation device. They are then accorded the same legal effect as handwritten signatures. A regular electronic signature is broadly defined as *data in electronic form that is attached to or logically associated with other electronic data and which serves as a method of authentication*. Both types of electronic signature are admissible as evidence but courts have broader discretionary authority in assessing the probative value of regular electronic signatures.

13. This stable legal framework should encourage the use of digital signatures and opens up promising market opportunities for those companies who provide the products and services that underpin the signature system. It will also raise awareness of the insecure nature of the Internet environment. The Directive does not specify any particular technology but the Commission has mandated European Standards bodies to work on specifications through the **European Electronic Signature Standardization Initiative.**[7].

### 1.5 Internal Market For Encryption Products

14. The EU wide availability of security products will increase users' trust in the information society. Security on-line is vital to building confidence, stimulating use of the Internet and driving the market for e-commerce. The ECU's Dual Use Regulation[8] (directly effective in all Member States from 29 September 2000) authorizes the export of most encryption products and services within the EU, and from the EU to ten designated countries including the United States.

---

[6] 1999/93/EC Directive on a Common Framework for Electronic Signatures http://www.ict.etsi.org/eessi/e-sign-directive.pdf

[7] European Electronic Signature Standardisation Initiative
http://www.ict.etsi.org/eessi/EESSI-homepage.htm

[8] Regulation 1334/2000 setting up a Community regime for the control of exports of dual use items and technology
http://europa.eu.int/eur-lex/en/lif/dat/2000/en_300R1334.html

15. Member States retain the right to impose additional controls on just one category of encryption products: crypto-analytic tools – the code cracking software used to test cipher systems. This is good news for e-commerce as commercially exploitable encryption technology is one of the key building blocks of the digital economy. The security market is currently mainly corporate but it will become mass as on-line security issues are given a higher profile.

16. Companies will no longer need a license for intra-EU cross border shipments of encryption technology. However, in response to the concerns of some Member States, a clause was drafted into the Regulation that allows them discretion in fixing the reporting requirements for such transfers.

17. The new rules also allow companies to get a Community General Export Authorization that allows most encryption products to be exported to ten "safe destinations" including the US, and is valid for export from any Member State. This Regulation makes life far simpler for US based companies with subsidiaries or partners in several member states and facilitates the service provided to customers of pan European services and networks.

### 1.6 Securing Consumer Rights Online

18. The unwillingness of consumers to buy on-line drives the security on the Internet debate. The **Brussels Regulation**[9] on Jurisdiction will provide consumers, subject to certain conditions, with a choice of jurisdiction in the event of a cross-border dispute - it enters into force on 1 March 2002. Legislative work is now focusing on applicable law issues. However, from the consumers' point of view, the time and money involved in litigation compared to the value of most products or services makes the legal route one of last resort. Consumers need access to quick, simple and effective redress through out of court type settlements like arbitration.

19. With this in mind the European Commission has launched the **E-confidence Forum**[10] to trigger a debate on e-commerce codes of conduct and on-line out of court dispute resolution. It has also been working with stakeholders to develop general principles that could be used by accreditation bodies in the EU Member States to endorse codes of conduct and trust mark schemes for shopping on the Net. Once complete, the principles may be endorsed by the European Commission. Codes of Conduct, trustmarks and effective dispute resolution combined with security technology should bolster E-confidence. More customers making more online purchases is good news for players in the Internet security market.

### 1.7 Securing Privacy On Line

20. Personal Data is a valuable commodity in the digital economy. Indeed the unique selling point of the Internet is arguably that you can better target your customer.

---

[9] Regulation 44/2001 on Jurisdiction and the recognition and enforcement of judgements in civil and commercial matters
http://europa.eu.int/eur-lex/en/lif/dat/2001/en_301R0044.html

[10] E-Confidence Forum
http://econfidence.jrc.it/default/show.gx?Object.object_id=EC_FORUM000000000000000D

However there is a delicate balance to be struck between proactively offering targeted goods and services, and invading privacy. The EU solution to securing personal data is a comprehensive set of rules enforced by independent national data protection authorities and known as the **Data Protection Directive**[11] (deadline for national implementation October 1998). The Directive requires the European Commission to assess the adequacy of controls put in by third countries before allowing transfers of data outside of the EU.

21. The United States Safe Harbor program[12] is a response to this requirement and was agreed by the Commission in July 2000. Companies that abide by Safe Harbor obligations must tell customers why they are collecting personal information, how they intend to use it and whether they will transfer it to third parties. Data subjects have to be given the chance to say no; and must say yes if the data is very sensitive. Their consent is required before the data can be transferred on to other parties and they must be allowed access to their files.

22. In 2001 the Directive and Safe Harbor are up for review. Legislation can provide a framework but the working solutions to data privacy have to be provided by industry through technology. This brings us back to the points mentioned with regard to the debate on cybercrime particularly with regard to solutions that hide the user's identify. The market to secure personal data in an on-line environment is set to grow fast. Already technologies and services such as cookie killers, proxy servers, anonymisation software, email filters, infomediaries and site labeling are driving the market. Data privacy legislation is also a driver – if companies cannot guarantee privacy they cannot trade effectively. They will be customers of the security services sector.

### 1.8 Securing Intellectual Property On-Line

23. The EU is in the process of agreeing a **Copyright Directive**[13]which will make cross-border trade in copyright-protected goods and services easier, with particular emphasis on "new" Information Society products and services. The new Directive, once adopted and implemented, will allow copyright holders to secure their works from unauthorized distribution over the internet. This should drive forward the market for security solutions in the digital rights management market

### 1.9 Securing Payments On-Line

*24.* The European Commission has proposed a three-year **Action Plan on Preventing Fraud**[14] and Counterfeiting of non-cash means of payment. The initiative,

---

[11] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data
http://europa.eu.int/comm/internal_market/en/media/dataprot/law/index.htm
[12] Safe Harbor
http://www.export.gov/safeharbor/
[13] Proposed Directive on copyright in the information society
http://europa.eu.int/comm/internal_market/en/intprop/intprop/news/601.htm
[14] Communication 2001/11 on a fraud prevention action plan
http://europa.eu.int/comm/internal_market/en/finances/payment/fraud/cardfraud.htm

adopted in February 2001, has yet to be approved by the European Parliament and the Member States. It aims to crack down on the growing problem of fraud and counterfeiting on cards and other non-cash means of payment widely used for cross-border transactions.

25. According to the Commission fraud grew by approximately 50% last year and a large proportion of that increase concerned payments made by phone or across the Internet. Tackling the problem is principally the responsibility of the payment systems industry but the European Commission sees its role in establishing systems to ensure better information exchange and stronger cross-border co-operation.

26. The Action Plan calls on the payment industry to provide the highest economically viable level of security for remote electronic payments by mid2002 at the latest. The Commission plans in addition to set up a Forum on security of payment products. This move should be followed in conjunction with the eEurope Smart Card initiative described in section 10. The demand for secure cross border payment systems, and services and products that go with them, is far from satisfied. As more customers are encouraged on-line that demand will grow still further.

### 1.10 Conclusion

27. An understanding of the threats, opportunities and compliance requirements presented by these developments in EU policy and regulation is essential to formulating successful business strategies aimed at entering and expanding in the region's Internet Security market. This short paper has tried to highlight the most important developments and has focussed on what is to come rather than what is in place now. For more information on how these developments might shape the market for your specific product or service please contact the Commercial Service at the United States Mission to the European Union.
Brussels.ec.office.box@mail.doc.gov

# 2 Austria

# 3 Belarus

At present, Internet Security in Belarus is developing faster than M-commerce. The list of major Internet security products and services available and not available in Belarus follows:

| | | | |
|---|---|---|---|
| Authentication | Yes | Virtual private networks | Yes but very few |
| Authorization | Yes | | |
| Administration | Yes | Intrusion, detection and monitoring | Yes |
| Secure transactions | almost N/A | | |
| Firewalls | Yes | Knowledge management | almost N/A |

| | | | |
|---|---|---|---|
| PKI | No | Security assessment tools | Yes |
| Encryption | Yes | Data warehousing and information | Yes, a little |
| Smart Cards | Yes | | |
| Content Screening, Antivirus and mobile code | Yes | Enterprise security | Yes |

The key player in this sector is the Government of Belarus. State Center on Information Security belonging to the Security Council of Belarus has been authorized to control the entire Internet Security field on behalf of the Government. The Center drafted a law on Electronic Document, which was then passed in January, 2000. This law is the major document regulating Internet Security issues in Belarus. More information can be found at http://ncpi.gov.by/eng/indexeng.htm

## 3.1 Statistical information

### 3.1.1 Some Internet Security-related statistics follow:

Utilization and penetration of the Internet. – about 150 000 – 200 000 users of Internet in Belarus.

### 3.1.2 E-commerce

Online purchases are very low in value. Almost all Belarussian internet shops (approximately 100) are grouped under www.shop.by Their total daily revenue in September 2000 was only $1500.

## 3.2 Contact information

JV IBA
Vitaly Nikulenko, Director of Internet Division
phone: 375 (17) 217 3390
mobile: 375 (29) 634 5384
fax: 375 (17) 217 3323
e-mail: vitalyn@iba.com.by

Ivan Petrovich, Director of Internet-forum
Phone: 375 (17) 285-2141, 285-6923, 224-2015
e-mail: Petrovich@nsys.by

### 3.2.1 Internet Providers in Belarus

Open Contact
Andrei Ivanov, Director
Belarus, Minsk, 220004, P.O. Box 286
phone: 375 (17) 211-0121,
fax: 375 (17) 211-0122
Internet: http://www.open.by
E-mail: webmaster@open.by

BELPAK (state owned provider)
Yuri Galyakevich, Managing Director
Belarus, Minsk, 220030, Engels 6,
phone: 375 (17) 217-1459 or 217-1460
fax: 375 (17) 227-1967
Internet: http://www.beltelecom.by
E-mail: sso@mail.belpak.by

Belresursmarket
Valeri Petrinich, Managing Director
Belarus, Minsk, Brestskaya 18-406
Phone: 375 (17) 277-4140, 277-4458
fax: 375 (17) 277-5043
Internet: http://www.brm.by
E-mail: general@brm.by

Network Systems
Alexei Kolb, Managing Director
Belarus, Minsk, 220013,
Surganova 37/4, office 120
phone/fax: 375 (17) 283-1711, 283-2467
Internet: http://www.nsys.by
E-mail: info@nsys.by

BAS-NET
Belarus, Minsk, Akademicheskaya 25
phone: 375 (17) 284-2095, 84-0722
Internet: http://www.bas-net.by
E-mail: mahaniok@bas-net.by

UNIBEL (state owned)
Belarus, Minsk, 220088, Zaharova 59
NIkolai Listopad
Phone: 375 (17) 210-0250, 210-0581
phone/fax: 375 (17) 210-0099
Internet: http://www.unibel.by
E-mail: sokol@unibel.by

SOLO
Belarus, Minsk, 220007, Kropotkina 44-1105, P.O. Box 31
Vladimir Ivashkevich, Director
phone/fax: 375 (17) 234-8164, 283-2979, 239-1387
Internet: http://www.solo.by
E-mail: market@solo.by

InfoNet
Belarus, Minsk, Skariny Av. 11-662
phone: 375 (17) 210-5800, 210-5811
Internet: http://www.infonet.by
E-mail: belinfonet@infonet.by

AviLink
Belarus, Minsk, Knorina 1/3, office 46.
Phone: 375 (17) 211-3925
Internet: http://www.idlab.com.by
E-mail: webmaster@idlab.com.by

GlobalOneBel
Vladimir Korseko, Director
Belarus, Minsk, 220002, Varvasheni 73-703
Tel 234-5924, 283-1459 (8)
Fax 210-1937
Internet: www.global-one.by
e-mail: sales@global-one.by

GT Provider
Sergei Fishbein, Director
Belarus, Minsk, 220050, Revolutsionnaya 24/a-5
Tel. 206-5561
Tel/fax 223-9512
www.gtp.by
e-mail: office1@gtp.by

Delovaya Set
Sergei Poblaguev, Director
Belarus, Minsk, 200030, Sq. Svabody 17-711
Tel/fax 2065060, 206-5006, 213-1933, 213-2453
Internet: www.bn.by
e-mail: psi@bn.by

# 4 Belgium

## *1. Summary*

The ICT Security (ICTSEC) market in Belgium has rapidly developed since 1997 and is predicted to sustain growth of about 30 to 35 percent during the years ahead. This growth pertains especially to firewalls, intrusion detection software, Virtual Private Networks (VPN), digital certificates, and Public Key Infrastructure (PKI) market

segments. Of the aforementioned applications, firewalls, intrusion detection software, and VPNs are already being used in large companies. There is new growth in the Small and Medium Enterprises (SME) market, made possible by the recent implementation of Asynchronized Digital Subscriber Line (ADSL) technology in the Belgian telecom network, resulting in the availability of affordable bandwidth.

According to a Belgian value-added distributor of security products, about 150,000 Belgian SMEs are ready to invest in ICTSEC products and services. Belgium imports these products mainly from Israel and the United States. The large Internet savvy companies, deeply immersed in e-commerce activities, are implementing all-encompassing Internet security systems with high-end security features such as digital certificates and PKI technologies. In general, about three fourths of Belgian companies have implemented some form of security measure. The most popular form is anti-virus software with 97 percent market penetration and the second is firewalls with 67 percent. The applications of more complex PKI or VPN solutions are less popular and the market penetration is less than 10 percent.

## *2. Market Overview*

*Market Trends*

The current growth of the Belgian ICTSEC market is made possible by the emergence of e-business. On the other hand, security is an e-business enabler; future growth in e-business is dependent upon the development of a secured IT-infrastructure. A majority of Belgian companies are well-aware of the fact that e-business activities run a high security risk, therefore they have included network security in their business plans. However, in most cases the execution has not been carried out. Large companies need to review the purpose of information security with their business departments and set up processes of measuring and managing risk.

A year or two ago, a Belgian company's IT department concentrated on the security of the internal company network against attacks from the outside. In general, internal users were regarded as "friends" and external users as "potential enemies". At that time, the available activities were limited to brochureware for Internet sites and e-mail services for internal users. Firewalls were used to give access to "friends" and prevent "potential enemies" from entering. Today, companies have been forced to provide access to their internal networks to an ever-increasing number of outside users, including customers and partners. Outsiders can obtain access to the company network system to place and track orders, to request information and check stocks. The company network becomes a part of the worldwide network, and this endangers the company's critical information and applications. The result is that firewalls are no longer enough. The traditional network security must be upgraded with tools enabling secure use and distribution of digital content which are integrated in broader and preferably automated security solutions.

Belgian corporations recognize that the Internet disperses most viruses. Corporate environments are migrating to server-based and gateway anti-virus implementations because most viruses are network and/or mail-based. Large enterprises with multiple sites are demanding a console for managing thousands of anti-virus applications on distributed servers. Active content is the new security threat transmitted via Internet, therefore, proactive Internet content security has become important.

Another boost to the Internet product and services market and the ICTSEC market is the development of the Belgian government's ambitious e-government plan. Announced at the end of 2000, this plan will be introduced gradually, but should become partly operational within a year. The e-government plan entails the development of a central government digital platform to which national, regional, provincial, and local administrations will be seamlessly connected. In addition to the new platform, the back office and front office will be reorganized, including the introduction of a portal site and PKI functionality that offers unique personal services to citizens in the front office. This BelPKI-project mainly covers the creation and certification of a Belgian e-ID card. The development of e-government is based on a public/private partnership, and companies will be invited to participate in a vast consultation. According to a press article, the Belgian Post Group, formerly the Belgian Postal Service (BPG) is a possible manager of the portal site. The BPG has currently set up four subsidiaries, two of which are involved in e-services and e-business solutions. However, another prospective manager, Intrasoft International (a Greek-Belgian IT company) is also being considered.

The market growth for security systems in general will predominantly come from Internet-savvy SME's. In Belgium, 73 percent of the country's total employment is made up of SMEs, representing 66 percent of the country's turnover. The top 5000 telecommunications companies involved in finance, retail, and technology and government organizations are the target market for high-end security solutions. Developing areas of product applications include co-location, web hosting, and data center. In addition, the locally established ISPs, ASPs, and MSPs (Managed Service Providers) are offering a virtually untapped market for large numbers of ICT security systems.

*Market Players*

The ICTSEC market players in Belgium are principally foreign brands (Israeli, American, and European). The solutions include security appliances, hardware-based security devices, and software-based counterparts. The current leader in the access control market is Check Point, an Israeli company whose firewall software has an estimated market share of 90 percent. Other firewall brands include Alteon (plus load balancing), Axent, Fore, Lucent, Network Associates, Nokia, Watchguard, Sonicwall, and Netscreen (plus VPN). Check Point is currently challenged, especially in the SME, ISP, and ASP (Application Service Provider) markets. Competitors such as Netscreen offer chip-based solutions, which perform at wire-speed and are easy to install. Prevailing intrusion detection brands are ISS and Computer Associates, and content screening and anti-virus market players are Content Technologies and Trendmicro. Authentication products on the market include RSA Security, Rainbow, Aladdin, and Vasco. The leader in Internet monitoring, reporting, and managing

traffic is Websense. Cisco is a major supplier in integrated security solutions, whereas Computer Associates is involved in high-end security solutions against common threads, Business to Customer (B2C) Internet defense, and Business to Business (B2B) Trust Management.

Local players include importers and value-added distributors of the aforementioned foreign ICTSEC hardware and software. Acting as ICTSEC service organizations, their activities focus on IT network integration and consultancy services. The solutions that are offered by these companies generally include top of the line hardware and software products of American origin. The supported platforms include client server systems based on LINUX and Windows NT. These value-added distributors will continue to introduce products of leading vendors, which specialize in the fast growing segments of security and management of the Internet industry. The distributors typically have a network of value-added resellers or partners, generally ISPs, ASPs, system integrators and software houses in Belgium and Luxembourg.

## Leading distributors focusing on ICTSEC

AB Computers is a value-added distributor of computer hardware and software infrastructure, web environment and network security. Its network security product range includes Check Point (Firewall and VPN), StoneSoft (Firewall and Web Server & Web Cache Server Products), SonicWall, and Aladdin's eSafe and eToken products.

ACAL Belgium is a member of the ACAL PLC group with offices in Belgium, France, Germany, Italy, Netherlands, Norway, Sweden, Finland, UK, and the USA. ACAL Security & IP Multiservices Belgium is a value-added solution distributor that sells products and solutions through indirect sales channels such as resellers, VARs, Original Equipment Manufacturers (OEM), and systems integrators. Its security product offerings include Axent, SonicWall, CheckPoint software, Nokia, Intrusion.com, Cisco, Alladin, WebSense, and Stonesoft.

Comsol is a service organization and a leading Benelux distributor of high-end software and hardware for Intranets and for the Internet. Comsol's current partners in network security include Content Technologies, ISS, RSA Security, Trend Micro, WebSense, Check Point, F-Secure, Nokia, Stonesoft, and Watch Guard. Comsol experts carefully select suppliers by reviewing their past commercial and technical performance as well as their future plans.

DCB is a leading Belgian value-added distributor for quality Internet security products. It offers a high level of customer support and knowledge transfer. Its products include firewalls, thin Internet Servers, access control, Layer 7 Switching, e-mail scanning, traffic shaping/load balancing, intrusion detection, remote scanning, and remote access security. DCB also provides outsourcing services of Internet security.

Peapod Distribution in Tervuren, Belgium is the home office for the Benelux markets of the Peapod Group. One of Europe's leading e-software and e-services providers,

the Peapod Group equips Internet and enterprise networks with complete management security. Peapod has a vast customer base including the public, finance, utilities, retail, manufacturing, and pharmaceutical industry sectors.

Switchlink is an integrator of high-end data networks and provider of a range of products and services to the enterprise, carrier, and e-business markets. Its e-business infrastructure product line is focused on security with Netscreen (firewall and managed security VPN), load balancing with Foundry, and Packeteer provides traffic monitoring, shaping, and application performance enhancement. Recently, Switchlink was partially acquired by Brussels-based Intrasoft International. Intrasoft supplies IT services in the Benelux to companies such as Worldcom, European Central Bank, European Commission, and European Parliament.

#### 4.1.1 Local Players

Belgium has an impressive number of strong ICTSEC producers. These companies are principally concentrating on market niches such as security of payments, electronic signatures, biometrics, application security middleware, and value-added services such as on-line security services and security portals.

Brussels-based GlobalSign is a fast-growing international certification network, PKI solution provider, and a worldwide trust service provider. GlobalSign is acknowledged as an official Certification Authority for the European Commission. So far, the company has issued 3 million digital certificates. Moreover, it offers online services for creating and managing digital certificates, signed/sealed e-mail messaging, and for fully authenticated and confidential e-commerce. Globalsign develops flexible corporate PKI-solutions to all types of companies and offers applications such as m-commerce security, trust labels, and timestamping.

Keyware has pioneered the field of biometrics. Co-headquartered in Belgium and Woburn, Massachusetts, Keyware is a premier provider of intelligent biometrics and centralized authentication solutions for real-world business applications. Keyware has several divisions: Technologies & Solutions, Physical Access, Internet US and Internet EU, and Smart Card. Keyware licenses its technology to OEMs, System Integrators (SI), and ASPs. On January 16, 2001 Keyware and Gemplus (world leader of smart card based solutions for security, wireless and e-business applications) announced their partnership agreement to protect smart cards with biometric technology.

Ubizen is a leading e-security solutions provider in Belgium. Its principal product line MultiSecure provides secure e-business transactions and web portal access through policy-based application-level security. It also offers a managed security service, OnlineGuardian, and Professional Services combining consulting, deployment and support services with best of breed third party products.

Another player in the security product and services market is the Belgian branch of the Utimaco Safeware Group, the German producer of professional and certified IT security solutions. Utimaco develops and sells security solutions based on established standards for the mobile/desktop, network, e-commerce, and infrastructure market

segments. As a solution provider, Utimaco implements customer-specific security projects based on configurable standard products. Utimaco is an international player with 12 branches in 10 European countries, the US, Australia, Asia, and South Africa. Utimaco focuses on large national and international customers with complex security requirements such as government authorities, banks, and insurance companies. The Belgian Army uses a VPN solution from Utimaco for the satellite-based transfer of patient data. SafeGuard Easy and a secure triple DES process are used to encrypt this highly sensitive data and protect the patients of the Army's medical services.

Vasco is an American/Belgian global enabler of authentication, authorization, and administration security. Its security solutions range from the Digipass family of strong authentication products to the SnareWorks family of enterprise infrastructure software that provides Secure Single Sign-on, public key enabling, access control and entitlements, and web portal security. Headquartered in Chicago and Brussels, Vasco has more than 500 customers and 5 million end-users around the world. The company secures sensitive information and transactions in financial, government, education, healthcare, technology, manufacturing and telecommunications industries. Vasco safeguards e-business and e-commerce initiatives, mainly in protecting the transactions, information, and identity of users conducting online banking. Their activity secures the enterprise from the mainframe to the Internet, as well as securing remote access to corporate networks.

**Early Adopters of ICT Security**

The financial sector in Belgium was one of the earliest adopters of ICTSEC systems, resulting in numerous local initiatives for the banking sector. Banksys is the primary example in the field of secured payment products and services in the Belgian market. The use of electronic payment in Belgium is very popular. By end of 2000, during a normal Saturday, reportedly 2.8 million transactions were registered. The Banksys network, BANKNET, connects every ATM and point-of-terminal in Belgium with the operational service at Banksys.

Banknet has converted all networks to Internet protocol and has the lowest number of fraud-cases in the world. Banksys guarantees its clients a high level of safety in each stage of the electronic payment, from the entry of the PIN-code until the transaction data is saved. The company has also developed the first JAVA-based terminal, the C-ZAM/SMASH. Banksys plays an important role in the discussions of international standards in cash card-technologies, such as EMV and CEPS.

In 2000, Banksys launched Banxafe™, a solution that guarantees secure e-commerce and allows payment with Proton (an electronic purse smart card, cash card, or credit card that uses the bank's secret code). Banxafe was specifically developed by request and in close cooperation with the Belgian banks and the Bank Card Company. Banxafe is 100 percent compatible with the SET (Secure Electronic Transaction) international standard developed by VISA and Eurocard-MasterCard. Banxafe will be available to all bankcard users in Belgium in spring 2001. With around 250 Belgian businesses on the Internet, 20 percent have already signed a contract. In

addition, Packard Bell has concluded an initial strategic agreement aiming to equip all its computers with C-ZAM/PC card readers and a banxafe key (represented by a shopping cart) on the keyboard. This key will take Internet surfers directly to e-commerce sites where they can make secure payments using banxafe.

In 1994, the 5 largest Belgian banks established Isabel, a B2B electronic banking network that is now the largest certification authority in Belgium. One of the first B2B electronic market places in Europe, Isabel connects about thirty banks (including 15 foreign institutions) with more than 45,000 client companies through one multi-bank interface. The Isabel certificate, combined with RSA and Smart Card technology, is one of the most secure systems in the world for B2B e-commerce transactions.

The Belgian market has been chosen by PSINet to launch a European pilot project for its e-scan Managed Security Services, a distributed total solution for outsourcing of e-mail security. PSINet is providing a centralized super-filter, in which the electronic mail is analyzed, filtered, treated, and subsequently forwarded or not forwarded to the addressee. The service e-scan is part of their "Smart Global Office" offering that also includes VPNs. Within 3 years, PSINet hopes for 1500 e-scan clients in Europe or 200,000 users (300 clients in Belgium). The e-scan service was developed in cooperation with Activis, the European Managed Security Services specialist.

## *3. Competitive Analysis*

As a highly developed market economy, the Belgian market is heavily reliant on international trade. The country's GDP is dominated by the service sector (70 percent of GDP), followed by manufacturing (25 percent), and agriculture (2 percent). Exports account for more than 74 percent of Belgium's GDP, making it one of the highest per capita exporters in the world. In addition to its own exports, Belgium functions as a transit and distribution center for the rest of Europe. Its population of just over 10 million may not offer a large market in itself, but its location in the heart of Europe and its linguistic links with France, the Netherlands, and Germany increase its value in terms of potential market access.

In addition to their competitive and sophisticated nature, the Dutch, French, and German groups and their related consumer characteristics mark the Belgian market. At the business level, where price and technical factors are paramount, the language issue is not particularly significant. However, personal relationships between buyers and sellers can be influenced by the language factor, therefore it is important to carefully check claims of importers and distributors as to whether they cover the whole Belgian market.

State-of-the-art technology, quality, service, and price are determining factors for successful sales in the highly competitive Belgian market. All major international brands are active in the market. Immediate and reliable service is vital in hardware, software, and electronic information services sectors.

Market obstacles to ICTSEC products and PKI implementation include limited awareness of all security issues, minimal understanding of PKI, the complexity of installation and deployment, as well as a lack of multi-vendor interoperability. Yet PKI growth has been propelled by a number of factors, namely, the security for e-business which is currently a primary concern. Other factors include large-scale VPNs, secure e-mail, and storage of strategic applications for a web-based environment.

Belgium and the United States have enjoyed strong reciprocal trade relations over the years; Belgium ranks as the 9th largest trading partner of the United States. Belgium imported $11.3 billion from the United States in 1999 and is home to over 1,300 U.S. companies that play an active and important role in the economy. New-to-market U.S. suppliers of computer and network security products should carefully select a local partner or a local sales representative in the Belgian market. It is most important afterwards to maintain direct contact with local business partners in order to be informed about new developments in the market. The best prospects for U.S. suppliers include new generation hardware and software that increases availability, performance, and scalability of secured Web and e-commerce infrastructure. Server-based anti-virus and content security products are also promising market segments.

## *4. Statistical Information*

The Internet Market

It is estimated that 44% of Belgians currently have access to the Internet, either at home or in the office. 35.5 percent (600,000) Belgian surfers have already made an online purchase, an increase of 30 percent during the last five months. As far as on line activities are concerned, 22 percent of Belgians perform their banking transactions, 7 percent buy and sell shares, and 11 percent have looked for a new job on the web. Around 70 ISPs offer their services in Belgium and many offer free Internet connections. Operator related ISPs are Skynet (an affiliate of Belgacom merged with Infosources), Planet Internet and XS4All (KPN), UUnet (Worldcom), Itinera (Versatel), and Wanadoo (France Telecom). Cable operator related ISPs include Pandora (Telenet) and Chello (UPC). While all major international ISPs are accessible from Belgium, major international players such as AOL and Compuserve have low market penetration.

Percentages of private Internet use in Belgium are predicted to increase from 8,6% in February 2001 to 30% in 2003. At the end of 2000, 140,000 applications for ".be" address were registered and 41,509 addresses had been declared. In a recent survey by Internet Week, 77 percent of IT and e-business decision-makers in Belgium confirm that they will increase their Internet related budgets in 2001. Nineteen percent will keep their budgets at the 2000 level, whereas 4 percent are decreasing their investment levels.

*E-commerce*

Trade sources reveal that B2B and B2C transactions have had rapid increases during the last few months. The total e-commerce market in Belgium in 1999 was worth $186 million and is expected to grow to $13.8 billion by 2004. This growth will predominantly come from Internet-savvy SMEs. The SME sector in Belgium represents 73 percent of the country's total employment and 66 percent of the country's turnover.

According to a recent study by Insites (Belgian Internet market research bureau), during 2000, some 730,000 Belgians made a purchase via Internet, which represents 36 percent of the regular surfers. This shows an increase of 59 percent from 1999 when Belgium counted 460,000 e-shoppers. Online shoppers spent $ 445 million in one year, a very small fraction of the normal business channels. However, this does mean that the online turnover has increased by 40 percent in half a year. Travel ($ 111 million), financial services ($ 80 million), and computer hardware and software ($ 67 and $49 million) are popular online purchases. Together they make up 70 percent of the online sales. In all, 3.5 million orders were placed via the Internet, including 1.5 million books and CDs.

Insites expects that by the end of 2001, the cap of 1 million online buyers will be surpassed. On average, online purchases are still made by highly educated males, but the trend is changing. The increase in online purchases also comes from women who are trying online shopping for the first time. 64 percent of Belgian online surfers placed orders on Belgian sites, compared to 55 percent in the beginning of 2000. Reportedly, 100,000 surfers bought their presents during the holiday season.

According to a pan-European study, professional purchases by Belgians during 2000 totaled $93 million, and the average value of a professional purchase amounted to $140 (much lower than the European average of $305).

# 5 Bulgaria

## 5.1 Summary

Bulgaria has an Internet security market estimated at about $510 million, which is expected to have a steady growth of about 10 percent over the next several years. U.S. companies are market leaders with almost a 100 percent market share. Bulgaria has no companies that offer complete Internet security solutions, which is why end-users must contract with both hardware and software companies. However, with the increased use of e-commerce and Internet banking, the concern over Internet security will also increase. Therefore companies that will specialize in Internet Security solutions are expected to emerge.

## 5.2 Market Opportunities and Best Sales Prospects

U.S. companies working in the area of Internet security have an excellent reputation and are known as world technology leaders. There are no entry barriers or obstacles for the import of Internet security hardware equipment and software in Bulgaria.

U.S. companies that want to operate successfully on the Bulgarian market should consider appointing a local agent or distributor, who can not only sell the products but also provide excellent product maintenance and support, as services and support are an important part for the overall client satisfaction and especially given the fact that Internet security services and support market has excellent development potential.

The further development of the Bulgarian banking system and the real time bank settlement in particular, together with the development of Internet banking, e-commerce and on-line reservations will contribute to the development of Internet security. The pending law on e-documents and e-signature which is expected to be passed by the Bulgarian National Assembly will significantly contribute to the growth of the Internet security market, as the electronic transfer of documents will require additional and higher level of security.

At present, the biggest Internet security users in Bulgaria are commercial banks, the Bulgarian government and international corporations. However, since this is still a new and not very well-developed market, there is not much of an Internet security concern and many people still do not realize the damage which can be caused to them and their customers.

The following are the Internet security technologies currently in use in Bulgaria:

- Authentication
- Authorization
- Firewalls for secure transactions and virtual private networks
- Encryption
- Antivirus screening
- Enterprise security solutions

All of the existing Internet security technologies such as authentication, authorization, firewall for secure transactions and Virtual private networks, encryption, antivirus screening and enterprise security solutions are known and used in Bulgaria. However, the products in the following areas have the best sales prospects, where the highest market demand is expected:

Firewalls for securing Intranets and Virtual Private Networks

- Antivirus programs
- Encryption software
- Secure transactions hardware and software
- Enterprise security solutions

Cisco, Microsoft and Symantec are clear market leaders in offering hardware and software for Internet security, although the products of smaller companies offering cheaper products also have good market potential.

# 6 Czech Republic

## 6.1 Summary

Internet growth has been very rapid in the past several years in the Czech Republic. Between 1998-2000, the number of Internet users has grown by 240%. The majority of Czech companies have access to the Internet. Currently, 88% of 100 largest Czech companies and 61% of all small and medium sized companies have a web site. Leading companies have launched ERP (Enterprise Resource Planning) and CRM (Customer Relationship Management) systems and many of them now proceed with integration of these systems into e-business applications. Banking sector and state administration were the fastest developing IT sectors in 2000, followed by telecommunication and food processing industry. Investment for IT technologies reached $760 million, of which the banking sector spent $90 million, and state administration sector spent over $72 million for IT technologies. Also number of Internet home users has grown considerably, a fourth of all Czechs have an access to an Internet at home, compared to about 15% in 1999. Internet sales grew year-on-year by 600% in 2000, amounting to $2.6 million. The forecast for growth by 2003 is 25% Internet penetration and over $3 billion in e-commerce.

The Internet has started to become the most important business platform, enabling connectivity to all e-business players: customers, partners, suppliers, and employees. The first generation of e-business applications focused on navigation and speed, while the new generation demands security, reliability, availability, and performance. This brings enormous opportunities to companies delivering innovative solutions. Security solution could be handled as standalone product, as a security site, or fully integrated with e-business infrastructure management solution. The up-to-date solutions must include risk assessment, attack detection, loss prevention, and support key industry standards. Security solutions, that are part of the larger task of enterprise management are protecting infrastructure and power the e-business. The solutions securing the e-business include intrusion detection, administration, authentication and authorization, and VPN (virtual private networks). With seamless platform coverage, the solutions provide comprehensive, end-to-end security.

Companies, delivering security solutions, are holding considerable share of the IT market. Innovative solutions are built on up-to-date HW and SW platforms, and integrated with solutions available on market. Market for security solutions is very competitive and open also to small and mid-sized companies. Its international character forces companies to follow new trends and meet high standards, on the other hand enables them to offer their products internationally, to a very broad range of clients. Czech companies are holding very strong position on domestic and international market in delivering complete solutions that meet needs of individual clients. There is a great opportunity for U.S. firms to distribute their security solutions via local value added distributors or select local software developers to deliver solutions based on U.S. company’s security products. There are several examples of success of local software developers: during 2000, Sun Microsystem has purchased local firm NetBeans, that develops software solutions; Czech company Tiny Software

has become supplier of software solution for the U.S. Navy, and leading local firm AEC delivers security solution worldwide.

The Czech Republic closely follows all international trends in the data protection legislation. When developing a legislation framework, the EU directives have been followed. The Czech Act on Electronic Signatures, that came into effect in October 2000, implemented to a great extend the EU directive which should be implemented by all EU countries no later than July 2001. The certification practices framework is in a process of discussion and should come into effect by mid 2001.The following organizations participate in development of certification policy: Data Protection Agency, Security Information Service, Office for Public Information System, and the Association for Information Society. They cooperate with the European Electronic Signature Standardization Initiative and follow the EU framework for development of Public Key Infrastructure (PKI) certification practices.

While the legislation is in a stage of development, several Certification Authorities (CA) have already been providing their services to clients on commercial basis. During 2001, the government should decide whether there will be a specialized Office established, that would be authorized to form the Root Certification Authorities, audit and control them and enforce the Act on Electronic Signatures, or authorize some of existing commercial CA to become the Root CA.

## 6.2 Market Overview

The market for security solutions and services has been growing rapidly in the past year, following the fast development of IT and telecommunications. Leading sectors are banking and the state organizations, followed by telecommunications, food processing, and manufacturing of electronic components. Majority of local banks started in 2000 to offer e-banking services. State organizations, including Ministries, Parliament, and state administration offices are becoming accessible to public via Internet. The Czech Republic has been very successful in attracting foreign investment in the past years, due to good incentive policy. Foreign investment has enhanced building and implementation of large manufacturing plants and brought about needs for up-to-date management systems including security solutions and access to e-business.

The growth of needs has brought an opportunity for companies active in delivering security solutions and related services, such as system integrators, software developers, value-added distributors and application service providers. In the security sector, up-to-date information on methods, legislation and solutions is on a very high level. The sources of information are trade fairs, conference, specialized events such as company presentations, and Internet. Majority of companies are aware of the fact that the security solution is an on-going process that has to be continually developed. Complete firm’s security solution could be built in steps, from installation of firewall, VPN, anti-virus protection, further to include encryption, two-phase authentication, digital certification and PKI, and should be completed by intrusion detection, network monitoring, and performance measurement.

### 6.2.1 Market Segments

The following products are currently available on the market, as components of innovative security solutions:

- Firewall : firewall is the basic component for network protection from non-authorized users. There are the three types of firewalls: packet filters, application gateways and gateway based on the Stateful Inspection technology standard. Recommended solution includes combination of packet and application filters, or use of the Stateful Inspection standard. Firewall does not protect internal network from authorized users and from attack (virus) initiated inside the network. Anti-virus programs should be applied together with the firewall.

- Virtual Private Network (VPN): VPN provides safe communication with open networks, such as Internet. It enables safe communication with company branches, managers on business trip, company suppliers and clients. VPN solution provides encryption of communication channel and user authentication. Encrypted channel can be used for communication with individual computers. VPN has become a part of the firewall in up-to-date technologies.

- Anti-virus protection: a wide portfolio of anti-virus systems is being offered. Anti-virus systems protect an internal network in several levels: protection of individual work stations, protection of LAN servers, and database replication protection (e-mail). Complete protection is provided by integration of anti-virus system with firewall.

- Intrusion detection: the method of intrusion detection is based on server that controls and analyses network performance. An attack from outside or inside the network, as well as pre-attack probes are detected and firewall is re-configured in order to protect the network.

- Authentication: authentication method implements mechanism of user identification. Strong authentication, used in banking systems, requires two items to be identified independently.

- Encryption: encryption method is used for defining user rights. Encryption system protects network from outside and inside intruders, and enables to create private environment for individual user. Encryption systems range from off-line encryption (files encryption), disks encryption, to encryption keys of different lengths.

- PKI (Public Key Infrastructure): PKI is a method of identification and certification of individual user from large group of users. The PKI infrastructure is a complex solution that enables user identification and certification of his electronic signature.

There are over 12 local firms that develop security solutions targeted to certain group of clients. To meet client needs, the solutions combine several security methods (Firewall with anti-virus, VPN with encryption, VPN with PKI). Following are typical solutions available from local software developers, targeted to specific clients group:

- Firewall based solution for large, mid-sized and fast growing small companies, that need safe internal and external gateways. The solution, that is built on the Check Point Software Technologies (U.S. company) products, protects company network from external and internal attacks, provides user authentication, protects the network from viruses, enables centralized network management, and integrates with products of more than 200 partners. The solution supports platforms of Microsoft Win NT, Sun Solaris, HP and IBM servers and 3Com, Bay Network, Nokia and Xylan routers.

- VPN based solution for companies that want to use Internet via remote access (not using private network), companies that enable an access to their databases, mobile users or key business partners, and companies, that require IPSec standard for communication with partners. The solution includes firewall with gateway encryption, and encryption on the side of client. The firewall meets the Stateful Inspection standard.

- PKI based solution, targeted to large and mid-sized companies that require implementation of VPN according to the IPSec standard; companies that use token cards and are looking for next generation of authentication solution; companies that have large VPN for communication between gateways and clients. Certificate Authority is based on the Entrust PKI technology.

In addition, there is a range of security solutions, available on the market, targeted to mid-sized and large companies that have already implemented an infrastructure and need to improve its efficiency, or upgrade the security systems to a higher level.

### 6.2.2 Major trends

The market growth for security solution has been following the very fast development of IT sector. According to the European Information Technology Observatory 2000, the IT hardware market segment grew by 7.1% in 1999/2000 period, while software systems segment grew by 8.8% and the application software segment by 14.4%. The growth of application software segment is predicted to grow by 16.6% in 2001. According to IDC (International Data Consortium), an investment into software and service market is predicted to reach $820 million in 2001.

These figures reflect the growing needs for hardware, software and mainly for application software. Local companies have proved a very high qualification for development of application software, build on standard products, available on the market. U.S. products hold the leading position in all IT market segments. In the application software development, close partnership with manufacturers and software developers is essential. U.S. security systems often set up an international standard that has to be met in individual solutions.

### 6.2.3 Market drivers

Market is driven by rapidly growing needs. Leading companies, that have already implemented ERM and CRM systems or an information system, are looking for solutions that bring higher system efficiency and/or enable them to go to e-business.

Especially fast growing is the banking sector. Competing environment forces banks to broaden their services by offering e banking. The leading retail local bank, Ceska Sporitelna, will invest $250 million over the next three years for upgrade of information system. Small and mid-sized companies are realizing enormous opportunities brought by use of Internet and are implementing their systems for the e-commerce.

The IT market growth is supported by a very fast growth of telecommunication infrastructure, and by very well developed Internet access. Access to Internet is available via dial-up, leased lines, wireless connection and cable TV. Large and mid-sized companies use mostly leased lines and wireless connection, while small companies use the ISDN lines, or dial-up connection. Speeds from 64 KBPS up to 256 APBs are currently available. There are 19 large ISPs with international connectivity covering the majority of the market. Another 350 regional sub-ISPs resell the services of the large ISPs and provide Internet access for local calls. International access of individual ISPs is provided via the Neutral Internet Exchange node (NIX.CZ) that has been created by the Association of ISPs. In 2001, NIX.CZ will become a central node for Central Europe. It will enable ISPs to connect at the speed of 1 Gbps.

There is a growing number of ISPs that expand their services to become Application Service Providers – ASPs. Their services include a high-level security solution when communicating with clients.

### 6.2.4 Market obstacles

There are no significant import obstacles hindering the security market development. Imported SW and HW products, including encrypted software are not a subject of high duty rates or any import limitations on the Czech side.

High telephone tariffs and high cost of leased lines may cause some obstacles, especially for small companies or for home Internet users. The price is composed of an ISP charge and the call cost according to the tariff rate of the operator. The average IPSs' charge for an Internet connection of 64 KBPS speed is $12.5, while the operators access price for 20 hours of off-peak time is $55, for peak time the price increases to $110. The monthly fees for leased line services vary from $350 to $1,750 in relation to speed and service.

Low trust in Internet security is a serious obstacle that has to be overcome by increasing level of information on security methods and by adoption of laws. The Electronic Signatures Act, which came into effect in October 2000, was pre-mature and its application has been hindered by non-existence of provisions in execution. A discussion is carried on, initiated by the Data Protection Agency, the Office of Public Information Systems, and other interested parties, such as Certification Authorities and firms, developing security solutions. The Act should be fully implemented in mid-2001. There are seminars and workshops regularly organized, for banks, state offices and public, to inform on solutions and technologies of security systems. The country's largest and most popular IT trade show, Invex, devoted the 2000 exhibition to presentation of complete solutions for e-business. To increase trust into Internet shopping and safe payments, the project of Trust-me-zona was introduced during the Invex show. The project brought together telecom operator, Internet provider, HW

and SW importers, solution supplier, bank, e-shops and delivery firm. Payments are provided via virtual bank accounts, that the bank, involved in the project (Citibank), creates for the customers. Virtual account is based on real customer account at any other bank, and prevents from misuse of customers bank account number. Since its introduction, the project attracted over 20,000 customers, as well as several e-shops, offering their products (mostly books, CDs, flowers, and toys).

### 6.2.5 Legislation

The certification practices framework is in a process of discussion and should come into effect by mid 2001. A group of experts from the Data Protection Agency has prepared a policy framework that is available for discussion on the Internet. It has been based on ETSI TS 201 456 “Policy requirements for certification authorities issuing qualified certificates” draft and the following documents, valid in the EU: IETF RFC 2527 (Internet X.509 Public Key Infrastructure – certificate Policy and Certification Practices Framework, 1999), ITU-T Recommendation X.509/ISO/IEC 9594-8 (Information technology - Open System Interconnection- The Directory: authentication framework), FIPS PUB 140-1 (Security Requirements For Cryptographic Modules), and ETSI TS 101 862 (Qualified certificate profile). The policy framework deals with identification and authentication, operational requirements, general provisions (obligations, liability, financial responsibility, enforcement), security controls (personnel, procedural, physical and technical) and certificate profiles of the Electronic Signature Act.

### 6.2.6 Certification Authorities

There are tree leading Certification Authorities that provide their services on the Czech market. They issue several level of certificates that can be used for the following purposes: as electronic signature of electronic documents, for protection of electronic documents, for protection of document from content changes, and for client identification in electronic communication processes. Certification Authority (CA) issues certificate after the client proves his identity to the CA . In relation to identification process, the client can receive certificate CLASS 1 (basic level certificate without specific security mechanism), CLASS 2 (client identification sufficiently proved by documents that can be identified by third party, such as police), and CLASS 3 (the highest security level certificate, CA provides liability). Certificates validity is limited for certain time period and has to be renewed. CA has to keep and publish the Certificate Revocation List (CRL). Certificates that are currently downloaded from Internet and used in applications such as Microsoft Outlook Express are certificates on the level of CLASS 1. Higher level certificates can be issued only by CA that have been audited by security audit of an internationally recognized auditor. The I-CA, the leading local CA, has issued more than 100,000 certificates since 1999 and currently has 25-30,000 active clients (those, who renew their certificates regularly).

## 6.3 Competitive Analysis

The market for Internet security products is very competitive. The key factor is up-to-date design, that supports frequently used SW and HW platforms and integrates with solutions of wide range of technology partners, providing flexible solution for reasonable price.

Software products/security solutions are distributed by local distributors as a single product, such as anti-virus systems, data protection systems, cryptographic SW, hardware keys, or complete packages such as software packages for specified activities (systems for banking, secure electronic mail, chip card technology, authentication systems for IT network users). More often, local value-added resellers offer individually developed solution, built on imported security product of foreign firm, and offer it together with services such as network design and implementation. System integrators offer complete solutions to large companies, banks, and state administration offices. Internet providers deliver security solutions design to protect clients' Internet-connected network against intrusion as well as help the client to use the IP infrastructure as a private communication platform.

U.S. companies dominate the Internet security market. Local solution developers cooperate with the following leading U.S. technology partners: Check Point Software Technologies, Computer Associates, Informix Software, Intrusion Corporation, RSA Security, Trend Micro, Vasco, Rainbow Technologies and Tibco Software. Leading country's System Integrator, company APP, based its solutions of ERP (Enterprise Assets Management) and CRM (Customer Relationship Management) on products of U.S. firms BEA Systems and Siebel Systems. Good position on the market is also held by German (Braun Informationssysteme, Norman), French (Activcard), and Japan (Toshiba Information Systems) firms. Firms hold Strong position from Israel, who are well known as developers of software and hardware security solutions (Voltaire Advanced Data Security Ltd.)

## 6.4 Statistical Information

| | 1999 | 2000 | 2001(est) |
|---|---|---|---|
| *A) Connectivity infrastructure* | | | |
| Number of conventional lines | 3,500,000 | 3,900,000 | 4,100,000 |
| - business | 1,050,000 | 1,180,000 | 1,300,000 |
| - residential | 2,450,000 | 2,720,000 | 2,800,000 |
| 64k ISDN lines | 20,000 | 100,000 | 150,000 |
| Number of mobile lines | 2,000,000 | 4,321,000 | 5,800,000 |
| - Eurotel | 1,250,000 | 2,171,000 | 2,690,000 |
| - Paegas | 750,000 | 1,850,000 | 2,360,000 |
| - Cesky Mobil | 300,000 | 750,000 | |
| *B) Turnover in the telecommunication market* (million USD) | 1,944 | 2,400 | 3,200 |
| *C) Internet users* (percentage of population) | 8.4 | 15.2 | 26 |
| -people with Internet connection at home | 2.2 | 4.7 | 10 |
| -people with PC at home | 14.7 | 25 | 35 |
| *D) General Economic Data:* | | | |
| GDP per capita: 5,153 USD | | | |
| GDP growth: | | 2.8% | 3% |
| Inflation: | 2.1% | 4% | 4% |

## 6.5 Contact Information

### 6.5.1 Legislation

Data Protection Agency
Havelkova 22, 130 00 Praha 3
Tel: 420-2-2100 8442, fax: 420-2-8943, 2271 7682, e-mail: info@uoou.cz,
Karel Neuwirth, Chairman
www.uoou.cz

State Information System Office
Havelkova 22, 130 00 Praha 3
Tel: 420-2-2100 8234, 2422 0614
Fax: 420-2-2422 3177
Alexander Kratochvil, Chairman, e-mail: kratochvila@usiscr.cz
www.usiscr.cz

### 6.5.2 Certification

I-CA Certification Authority
Martinska 2/360, 110 00 Praha 1
Tel: 420-2-6619 8481, fax: 420-2-6619 8622, e-mail: info@ica.cz
www.ica.cz

AEC TrustCert Certification Authority
Vinohradska 184, 130 52 Praha 3
Tel: 420-2-6731 1402, fax: 420-2-6731 4326, e-mail: praha@aec.cz

www.trustcert.cz

KPNQwest Czecha CertificationAuthority
Generala Janouska 902, 198 00 Praha 9
Tel: 420-2-8108 1081, fax: 420-2-8108 1082, e-mail: info.cz@kpnqwest.com
www.kpnqwest.cz, www.kpnqwest.com

### 6.5.3 Leading Security Solutions Developers and Distributors

AEC, s.r.o.
Bayerova 30, 602 00 Brno
Tel: 420-5-4123 5466-7, fax: 420-5-4123 5038, e-mail: info@aec.cz
www.aec.cz
Activity: development of security software, anti-virus and data protection, data encryption, security protection of workstations, computer and communication networks

Askon International, s.r.o.
Vlastina 23, Praha 6
Tel: 420-2-2040 9652, fax: 420-2-2040 9655, e-mail: info@askon.cz
www.askon.cz
Activity: distribution of hardware keys (Rainbow Sentinel), software solutions (encryption key, digital signature) based on products of U.S. firm Rainbow Technologies

Cigler Software, a.s.
Rostislavovo nam. 12, 612 00 Brno
Tel: 420-5-4952 2511, fax: 420-5-4952 2512, e-mail: info@ciglersw.cz
www.ciglersw.cz
Activity: development and support of information systems for medium and small companies

Decros, s.r.o.
J.S. Baara 40, 370 01 Ceske Budejovice
Tel: 420-38-7312 808, fax: 420-38-7311 480, e-mail:info@decros.cz
www.decros.cz
Activity: distribution of wide range of security technologies and related services, based on Microsoft operating systems

DNS, s.r.o.
Videnska 744/2, 140 00 Praha 4
Tel: 420-2-61003400, fax: 420-2-6100 3402, e-mail: dns@dns.cz
www.dns.cz
Activity: Value-added distributor of products for servers, network and clients solutions, supported by wide range of services (pre-sales support, installation, servicing, system configuration, management)

PCS Software, s.r.o.
Na Dvorcich 18, 140 00 Praha 4
Tel: 420-2-4144 0902, fax: 420-2-4144 0940, e-mail: info@eko.pcs.cz
www.pcs.cz/pcssoftware

Activity: development, sales and servicing of data protection software, anti-virus programs, network protection

PER4MANCE, s.r.o.
Fisova 3, 602 00 Brno
Tel: 420-5-4521 5400, fax: 420-2-4521 3291, e-mail: pmalenak@per4mance.cz
www.per4mance.cz
Activity: design and implementation of information systems, system integration, security solutions, e-business solution
PVT, a.s.
Kovanecka 30, 190 00 Praha 9
Tel: 420-2-6619 8111, fax: 420-2-6849 313, e-mail: sales@pvt.cz
www.pvt.cz
Activity: outsourcing IS/IT, e-business application, development of network technologies; operation of authorized training centers and courses; PVT operates the I-CA Certification Authority

# 7 Denmark

# 8 Estonia

# 9 Finland

# 10 France

**10.1 France**

The Year 2000 has marked the time when France has completely caught up with Germany, England and Nordic countries in its adoption of the Internet. The dramatic rise in Internet use experienced since 1998, when the number of users went from three million to nearly eleven million, including four million homes, has created an ever-increasing concern among governments, corporations and individual users for the security afforded by this new medium of communication.

The French market for E-business reached $600 million in 2000. This represents a 310% growth from 1999. Seventy-three percent of the French SMEs are connected to the Internet and 40% have their own web site. Although more reluctant than their neighbors in performing on-line purchases the French are gradually overcoming the psychological barrier which consists in being willing to supply one's credit card information over the Net.

French large corporations have become fully aware that implementing an E-business strategy is essential to their success. However, the process of linking clients, suppliers and partners to one single network greatly increases the risk of someone tampering with vital corporate data. Consequently, expenditures in network security are anticipated to grow proportionally to the number of individuals or entities connected to a corporate network. Fifty-five percent of the French managers are very concerned by the security of their systems and 25% of them consider that this issue has become a top priority.

Whereas security concerns with respect to systems used to be primarily related to technical failures or acts of piracy within the organization, they are now focused on external threats. Ninety percent of the French large corporations consider computer viruses as the main danger to their information systems. Viruses are very difficult to anticipate and prepare for. Yet, they can cause tens of millions of dollars worth of damage to a company. This risk can best be illustrated by the "I love you" virus, which created havoc across the planet within hours.

French SMEs remain more vulnerable than large organizations to potential damage to their systems. Whereas major corporations can afford a Systems Manager, this is not the case for SMEs. Outsourcing would therefore represent an attractive alternative for them. However, this approach has not yet been implemented on a large scale.
Systems Managers make all decisions pertaining to computer security for 60% of the French corporations. They would therefore represent a primary target for a U.S. firm seeking to sell security-related solutions. In 20% of the cases, especially when the company is relatively small, the person to reach would be the General Manager. In order to be successful in the French market, American companies should always ensure that their products keep high standards of reliability and are properly translated into French.

Considering the dramatic growth of the Internet-security market, a large number of organizations, both French and foreign, compete for a share of the French market. These companies focus on products such as anti-virus systems, intrusion detection systems, Public Key Infrastructure (PKI) or Smart Cards offers. The most promising fields are anticipated to be anti-virus software, the Virtual Private Networks - Internet Protocol (VPN-IP), as well as firewalls and authentication (i.e. electronic signatures).

Since the Internet and its related products originate in the U.S., American firms that specialize in security tools are in an excellent position to capitalize on their know-how to generate high revenues in the French market, especially among SMEs.

## 10.2 MARKET PROFILE

Most French managers understand that the Internet is a determining factor in the success of their organization. About 73% of the French firms were connected to the Internet in 2000, a 13 percent increase from 1999. Among these firms, 40% have a web site while only 27% did in 1999. As France caught up with Germany and England in the creation of elaborate web sites, companies are becoming increasingly aware of the vulnerability of their systems to virus contamination and computer piracy. According to French computer review, "*Le Monde Informatique*," investments in security-related tools should increase dramatically in France. A primary concern for 47% of the managers interviewed is to increase the access to their web site as well as improve internal communications. Computer investments are therefore focused on complying with legal requirements (41%), client wishes (34%), new applications (32%), investment in new computer systems (27%), e-business projects (25%) and security issues (17%).

A survey conducted by consulting firm *Arthur Andersen* demonstrates that 55% of the corporate managers consider computer security as a major issue. It has become a top

priority for 25% of them, as Internet and computer security are gradually becoming synonymous. Opportunities for U.S. firms specialized in the security business are therefore excellent if they can provide French tools with appropriate tools.
The various types of protections provided by computer security firms include the following:

- Anti-virus
- Intrusion detection
- Public Key Infrastructure (PKI)
- Smart Cards
- Encryption
- Demilitarized zone
- Virtual Private Network…

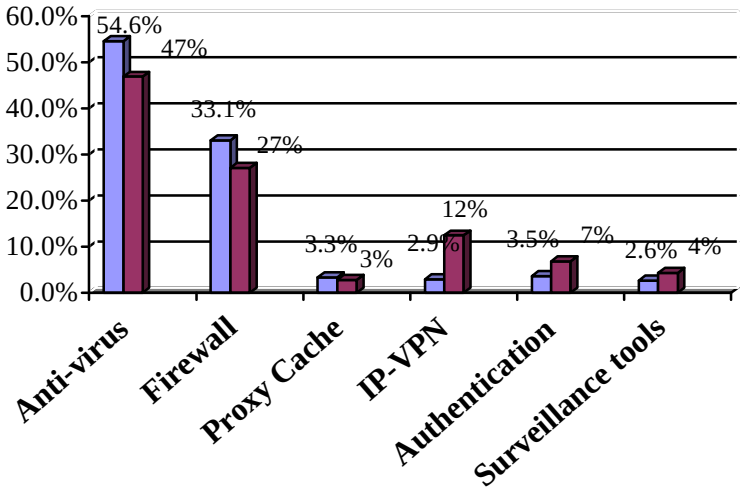
All these different options must be combined in order to get the best possible result. The mix is different for every company depending on the mainframe, the international environment, the number of suppliers and partners, or the distant access to the information.

A major challenge in France is that SMEs cannot afford a security team yet do not want to outsource this special service. However, they cannot generate business over the Net if their system is not equipped with proper security devices, especially when it comes to payment transactions. This is the reason why fine opportunities exist for systems security firms that can educate SMEs in the role that proper network security will play in their business.

## 10.3 BEST PROSPECTS

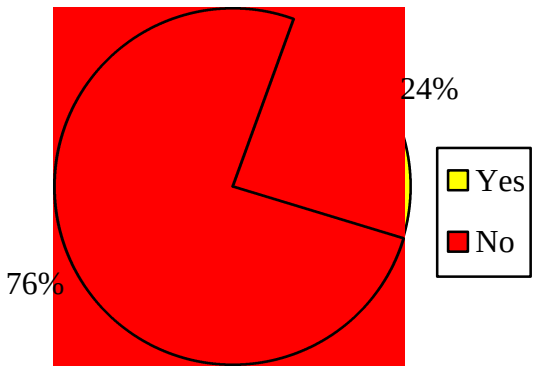
Managers views external threats to their systems as the most important, especially when it comes to dealing with viruses. Anti-virus devices and related firewalls are therefore taking an increasing part in the implementation of network protection devices. This may represent the most lucrative opportunity for U.S. firms.

**Market evolution in systems security products from 1998 to 2002 (forecast)**




As previously explained, outsourcing represents the most relevant solution for companies that cannot deal with security issues in-house. Although outsourcing represents an attractive option for SMEs, only large firms have been resorting to this approach, so far. Outsourcing is only used by 24.1% of the French firms. There is indeed a gap among many firms of medium size between the words and the commitment to enhance the security of their systems.

**Proportion of companies using outsourcing**




Source: *01Informatique*, September 2000

This attitude towards outsourcing is likely to create a handicap for SMEs, whose business is focused on B2B and B2C. They simply cannot enter this kind of activity without adequate security that can only provided by an external source. So far, 28% of companies of more of 200 employees have a team dedicated to computer security.

## 10.4 LEGAL FRAMEWORK

On March 17th 1999, the French National Assembly (Congress) voted a decree on the liberalization of Encryption. On March 13th March 2000, the French National Assembly adopted a law concerning Electronic Signatures. Computer companies are now waiting for the implementation of the law through decrees of application that should be published during the Year 2001.

The French government has postponed the vote of a law on "the Information Society" (LSI). This law needed revising which was in harmony with the development of new communication tools and the types of security that accompanies them (i.e. encryption, on-line security, etc.). The French government is also working on acts of legislation against "'cyberfraud," which is meant to address the issue of criminals tampering with the Net.

## 10.5 STATISTICAL DATA

***Repartition of E-business sectors***

| **Companies** | **Market Share** |
|---|---|
| Music / Literature | 31.3% |
| Bank / Insurance | 27.4% |
| Commercial firms | 19.4% |
| Software | 18.0% |
| Materials | 17.0% |
| Trips / Tourism | 11.9% |
| Toys | 10.3% |
| Stock Exchange / Finance | 9.20% |

**Source: *Journal Du Net*, November 2000**

Growth in number of Internet users in France

1996: 290,000 users.
July 1999: 3,500,000 users.
June 2000: 5,400,000 users (15.2% of the households are connected)

*Source: Net Marketing*

E-commerce market in France: $550 million in 2000.

Areas with the best growth opportunities are:

| | |
|---|---|
| Food: | +251% |
| Travel and Tourism: | +205% |
| Culture: | +158% |

In the last 6 months of 2000, French Internet users have principally bought books, CD's and DVD's (28%). 17% bought shares on the web.

73% of the French SMEs are connected to the Net.

40% have their own web site.

Percentage of SMEs connected to the Internet by sector of activity

| | |
|---|---|
| Industry: | 79% |
| Trade: | 72% |
| Public Buildings and Works Sector: | 56% |
| Transport: | 54% |

Use of the Internet in French SMEs in 2000:

| | |
|---|---|
| E-mail: | 73% |
| Information Research: | 64% |
| Clients/Suppliers relationship: | 51% |
| Financing research: | 3% |
| Bank account consultation: | 30% |
| Bank operations: | 17% |
| Others: | 22% |

SMEs intent on buying on-line in 2001

| | |
|---|---|
| Industry: | 11% |
| Trade: | 16% |
| Public Buildings and Works Sector: | 8% |
| Transport: | 15% |
| Services: | 13% |

Source: *Journal Du Net*

# 11 Germany

## 11.1 Summary

Germany is the largest ICT market in Europe, accounting for approximately 22 percent of Europe's ICT expenditures. Security software amounted to DM 750 million ($ 357 million) in 2000. Experts forecast this segment to reach DM 1.1 billion ($ 524 million) by 2003. Firewalls, anti-virus and encryption software account for the lion's share of the security software segment. Based on the anticipated growth in Internet usage, market potential for related security solutions is high.

## 11.2 Market Overview

### 11.2.1 Increased Demand for Internet Security Solutions

About 20 million Germans had Internet access in January 2001. Germany boasts about 1,000 providers of direct Internet connections. Growing acceptance of this

medium can also be evidenced by an increasing market volume of services for interactive computing, TV sets and internet access, which is projected to rise to € 4.4 billion in the year 2000, up from € 2.96 billion in 1998.

The German association for Information Technology, Telecommunications and New Media (BITKOM) is expecting considerable growth in software and services for Internet security. Internet security software sales amounted to around DM 750 million ($ 357 million) in 2000. This volume is expected to reach DM 1.1 billion 2003 ($ 524 million) by. The world-wide market for security software and services reached DM 11 billion this year and according to BITKOM will reach DM 19 billion ($ 9 billion) by 2003.

Anti-virus programs, firewalls and encryption-software account for the largest part of this segment. However, many decision-makers and IT administrators are still not prepared to invest large amounts of money into net security, which is partly based on a lack of information about available tools and how to use them.

### 11.2.2 Online-Shops: 90 percent are on the edge of the law

Developments in E-Commerce are not as positive as overly optimistic experts predicted earlier. Reasons are, among others, the lack of customer satisfaction with web-sites and potential security risks in data transfer.

A recent study researching over 100 online-shops showed that nearly all of these shops had security problems. A scan of net security revealed poor results: Only 5 percent of the researched networks were without faults, which means that hackers and crackers have virtually free access to a multitude of domains and shops. Potential attackers do not even have to be very skilful.

The majority of the surveyed internet-businesses have also neglected data protection, which has always been a big issue in Germany:

- 97% of online shops do not inform customers about data protection
- 86% do not ask customers for their consent when using their personal data
- 43% do not name the purpose for the data inquiry
- 93% do not guarantee that data will be deleted once the transaction is completed
- 63% do not inform customers about contract rights
- In 82% of the shops the General Terms of Business are not effective (because there is no consent from the customer to the General Terms of Business)
- 68% do not cover the costs for return delivery (and in doing so the Remote Sales law is ignored)
- 48% do not give a final price for the content of the shopping trolley
- 70% only offer one method of payment
- 44% do not name any personal contact on their Website

### 11.2.3 German Government Promotes a Safer Internet

“Safer Internet,” a task force of the Federal Interior Ministry provided a list of immediate measures for the improvement of Internet safety. This list contains advice on how to make planned attacks against Internet service providers more difficult or

completely deter. The German-language list can be found at www.bsi.de/ddos.html. One interesting example is the installation of short-term defense measures against Distributed Denial of Service (DdoS) attacks (such attacks actually happened in February 2000). The "immediate measures" listed by the task force describe four categories:

1) End-users should make sure that the installation of damage programs, which could be used in an attack against third parties, on their computers is impossible through the installation of virus scanners, secure web browsers and firewalls.

2) Internet service providers have to prevent the possibility of falsifying "Internet sender addresses," or at least make this considerably more difficult (prevention of IP Spoofing from package filtering). The implementation of package filters also protects the service-supplier against DDoS attacks. The necessary technology is available and can be implemented immediately without considerable cost.

3) Service providers should protect themselves through the implementation of package filtering, and the installation of programs, which automatically recognize attacks. They should implement emergency plans in the case of an attack, configure the computers safely and use open source software.

4) Content providers should ensure that the service-providers of their choice have IT security as an integral component of their service. They can constantly scan their database for attack programs and viruses and delete the so-called "active" content and thus eliminate unsafe end-user configurations.

Representatives of the large ISPs, manufacturers, associations, and government representatives from France, the Netherlands and the United States welcomed the Interior Ministry's initiative.

### 11.3 Competitive analysis

German customers tend to be more cautious in embracing E-commerce solutions than their counterparts in the United States. Research by Forrester shows that two-thirds of online shoppers in Germany choose to pay by invoice. This attitude has a somewhat schizophrenic effect on the market for Internet security solutions: while it obstructs faster developments in e-commerce, and thus limits potential, it also calls for a high degree of security for data transactions.

The German software encryption industry has a relatively large world market share and competition in the German market is increasing. The firewall software segment is highly competitive and may have reached saturation. Intrusion detection tools are in their early stages of development and offer good potential. (These tools raise an alarm as soon as there is an attempt to bypass security installations.)

### 11.3.1 Export Control of IT-Security products

Import and use of encryption products is not limited. Exports, however, are regulated by the Wassenaar-Agreement, in which more than 30 States agreed not to supply technology for the production of weapons to certain countries. Encryption products fall under the category of Dual Use Products. The Wassenaar Agreement has to be implemented via national legislation. Within the EU, this is based on the EG-Dual-Use Ruling NR. 1334, of September 2000.

## 11.4 Statistical information

Germany is the largest ICT market in Europe, equaling 22 percent of the Western European ICT market in 2000. Twenty-two million Germans are already using the Internet. The proportion of female users is increasing steadily and at the end of 2000 was at the 38 percent mark. 90 percent of German companies are on-line.

Around 6,49 million visitors clicked on online shop sites in December 2000. On average every German with Internet access surfed 17 times in December. In total, this amounted to around 8 hours and 15 minutes, about 10 minutes more than in November.

In the euphoria about B2B, B2C has been neglected. While there is growth potential in both sectors, B2B generates 80-90 percent of e-commerce revenues, and especially virtual marketplaces are becoming increasingly important. B2B is predicted to reach DM 230 billion ($ 110 billion) in 2004, compared with DM 4.5 billion ($ 2.1 billion) in 2000.

Exchange rate used throughout report: $1 equals DM 2.10

## 11.5 Contact information

BITKOM - Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.

(Association for Information Technology, Telecommunications and New Media)

Albrechtstraße 10
10117 Berlin
Germany
Phone: +49-30-27576-0
Fax: +49-30-27576-400
Email: bitkom@bitkom.org
Internet: www.bitkom.org

Founded in 1999, BITKOM represents around 1250 IT-Business with an annual turnover in total of DM 230 billion and nearly 800,000 employees.

Bundesamt für Sicherheit in der Informationstechnik
(Federal Office for IT Security)

Godesberger Allee 183
Postfach 20 03 63
53133 Bonn
Germany
Phone: +49-228-9582-0
Fax: +49-228-9582-400
Internet: www.bsi.de

Bundesverband der deutschen Industrie
(Federation of German Industries)

Breite Straße 29
D-10178 Berlin
Phone: +49-30-2028-0
Internet: http://www.bdi-online.de

U.S. Office:
Representative of German Industry and Trade
1627 I Street, NW, Suite 550
Washington, DC 20006
Phone: (202) 659-4777
Fax: (202) 659-4779
Email: info@rgit-usa.com
Internet: http://www.rgit-usa.com

Deutscher Industrie und Handelstag
(Association of German Chambers of Industry and Commerce)
Breite Strasse 29
D-10178 Berlin
Germany
Phone: +49-30-203080
Fax: +49-30-203082111
Internet: www.diht.de

German-American Chambers of Commerce in the United States of America:
Atlanta http://www.gaccsouth.com/
Chicago http://www.gaccom.org/
Los Angeles http://www.gaccwest.org/
New York http://www.gaccny.com/

Embassy of the Federal Republic of Germany
http://www.germany-info.org/f_index.html

U.S. Commercial Service contacts in Germany:

E-Commerce:
Mathias Koeckeritz
Commercial Specialist
U.S. Embassy
Neustaedtische Kirchstr. 4-5

D-10117 Berlin, Germany
Phone: +49-30-8305-2731
Fax: +49-30-2045-4466
Email: Mathias.Koeckeritz@mail.doc.gov

Software:
Doris Groot
Commercial Specialist
11.6 American Consulate General Munich

Königinstr. 5
D-80539 München, Germany
Phone: +49-89-2888-749
Fax: +49-89-285261
Email: Doris.Groot@mail.doc.gov

# 12 Greece

# 13 Hungary

## 13.1 Summary

From Hungary's total population of 10 million people, there are about 600,000 to 800,000 regular internet users. Low internet penetration (about 7 percent) is mostly due to high phone rates, relative to GDP per capita. These high rates, however, are expected to decrease with the further liberalization of the Hungarian telecommunications market scheduled for January 1, 2002.

B2C e-commerce amounted only to $ 3.5 million in 2000. The slow increase in B2C is due to the low Internet penetration that is expected to increase to 9 percent by 2003 and 12.5 percent in 2005. On the other hand, the rise in online banking will be slower than internet penetration. B2B e-commerce reached $ 11 million in 2000 and is estimated to reach $ 53 million in 2001 and $ 303 million in 2002. Awareness and ability to deal adequately with security threats through the Internet is not sufficient even with the current systems employed by some banks and financial institutions.

The Hungarian "Law on Digital Signature" is expected to be passed by the country's Parliament by June 2001. This law would speed up the spread of Public Key Infrastructure (PKI), and software that is related to digital signature will be one of the best sales prospects besides single sign-on authentication/authorization, content screening and antivirus software products.

Currently U.S. companies have about 70 percent country market share for internet security products. There is practically no domestic Hungarian competition. Third country competitors are: Active Card (France), Baltimore (Ireland), Check Point Software Technologies (Israel), Entrust Technologies (Canada), nCypher (U.K.). Brokat (Germany), Secude (Germany), Sonera Smart Trust (Finland) and Chrysalis (Canada).

Key competitive factors are: price and reliability. Local experts suggest that U.S. companies be flexible with pricing not using their global price list in Hungary. The same sources maintain that it is essential to have a Hungarian partner, a VAR or system integrator. They also recommend establishing a representation office or a Hungarian subsidiary to coordinate indirect sales.

## 13.2 Market Overview

Generally, it can be stated that awareness of internet security threats is not so widespread in Hungary, with the exception of some major banks and multinational companies. Customers of internet security solutions come from the following sectors: banking, telecommunications, government, pharmaceutical, oil & gas industry and IT. Small- and medium-size enterprises try to solve security issues in-house without using the consultancy and professional service companies specialized in security solutions. This state of affairs is expected to change with the increased growth in internet users. This should change more markedly after the further liberalization of the Hungarian telecom market scheduled for January 1, 2002. Currently high phone rates hinder the more rapid increase in internet users and "telecommuting" is not widespread except with some multinational companies. According to some experts the increase in the demand for internet security products will be continuous but not rapid.

### 13.2.1 Authentication

In 95 percent of the cases authentication is based on a password. The rest of the market uses token card solutions such as "Secure ID" of "RSA Laboratories (U.S.) and "Crypto Card" of Active Card (France) with RSA being the market leader. The use of smart cards in authentication is still in the initial phase in Hungary. There are some efforts to introduce finger print recognition in authentication. Guardware Systems Ltd. founded in 1999 in Budapest by an international group of investors has developed a fingerprint recognition technology by retaining innovations from previous Hungarian companies. Biometric security from Guardware Systems is based on advanced fingerprint recognition algorithms ensuring high and reliable performance and a durable optical scanner equipped with a unique biosensor. This biosensor - protected by international patents - recognizes and rejects finger surrogates with which intruders may attempt to compromise the system. The company is in an aggressive marketing campaign to attract the high-end markets demanding maximum security. With some banks and broker companies PKI based authentication solutions can be found as well. The single sign-on solution providing authentication/authorization to several parts of the system with one log-in is in an initial phase. There might be only a few implementations in Hungary but this area is considered to be a best prospect for U.S. companies.

### 13.2.2 Authorization

The access to a database or IT system resource, any right to use it or modify it is managed by the market leaders of Windows NT4, Windows 2000 of Microsoft, UNIX and Trusted Solaris of Sun. In case of database management systems, Oracle, Informix, Sybase and SQL Server of Microsoft are the market leaders. Cisco also has

a dominant market share supporting the following authentications, authorization and accounting (AAA) protocols: TACACS (Terminal Access Access Control Server) and Radius. Internet Service Providers, telecommunications companies and banks mostly use these solutions. The market of consulting services concerning authorization is fairly saturated. Besides the Big Five consulting companies, Hungarian system integrators (Montana, Synergon, Compaq, debis IT services Dataware, Proware, ) are competing with each other.

### 13.2.3 Public Key Infrastructure (PKI)

Netlock Co.Ltd. is the first and only one public Hungarian certification authority with two main activities: issuing digital certificates and PKI integration. Its Certification Practice Statement (CPS) is accepted by the Hungarian Chamber of Public Notaries and already conforms to the future Hungarian "Digital Signature Law" expected to be passed soon by the country's Parliament. Interestingly this company is one of the main consultants to the Hungarian Government of this aspect of Internet security.

X.509[15] certificates issued by NetLock Limited

| | |
|---|---|
| Personal | Issued to individuals, the certificate contains their personal data. |
| Business card | Issued to individuals working for any organization It contains customers' as well as organizational data. |
| Organizational | Issued to organizations, containing organizational data. While the use of personal and business card certificates enables the recipient to identify the individual who signed the document, organizational certificates provide information on the organization but do not reveal the signer's identity. |
| SSL[16], WAP[17]-Server | Issued to servers or WAP servers providing Secure Socket Layer (SSL) that creates a secure channel between the server and the client computer enabling its users to handle sensitive personal information (e.g.: credit card number) over the Internet. |

Trust levels of NetLock Limited's certificates

| | |
|---|---|
| Class A | The issuance of the certificates requires the necessary documents to be notarized. |
| Class B | The issuance of the certificates requires the customer's personal presence and submitting the original copies of the necessary documents |
| | |
| Class C | The issuance of the certificate requires a copy of the necessary documents. |

[15] International standard that describe the form of an electronic certificate
[16] Secure Socket Layer enables encrypted communication between a computer server and client
[17] Wireless Application Protocol enables communication on wireless networks

Another Hungarian company, ProfiTrade 90 has also developed its own Certificate Authority product, "jSure" being compliant with the X.509 international standard of the International Telecommunications Union (ITU) as well as with Secure Electronic Transaction (SET) and Identrus infrastructure. As "jSure" is implemented in Java, a platform independent programming language, the jSure application can run on any infrastructure.

Foreign Certification Authority (CA) service providers and PKI vendors try to enter the market such as VeriSign (U.S.), Baltimore (Ireland), Entrust Technologies (Canada), Sonera Smart Trust (Finland), RSA Laboratories (US). From time to time there are tenders (to test the market and prices) issued by telecom companies (MATAV), banks (GIRO, OTP) and the government but in most of the cases, the tenders are declared unsuccessful. Currently there are few sales; but with the relevant law on digital signature expected to be in place soon, companies contemplating PKI could create a market. All Hungarian market players interviewed agreed that PKI can be a best sales prospect in a few years time.

### 13.2.4 Administration

The following application packages are mostly used: "Open View" of HP, "Unicenter" of Computer Associates, "Patrol" of BMC, "Tivoli" of IBM, and Cisco Secure.

### 13.2.5 Secure Transactions

In Hungary, the Inter-Europa Bank was the first bank to use Secure Electronic Transaction (SET) when introducing e-banking in 1998; but it stopped operation in 1999. Some banks buy the products of Brokat (Germany); but there are Hungarian companies developing SET based applications i.e. "Java Merchant with SET" of ProfiTrade 90 Co Ltd. Being an international standard, SET developments are regulated and supervised by a vendor-independent international organization (founded by Visa and Master Card) called SETCo. ProfiTrade 90 was one of the first registered companies in Europe starting SET development and currently the only one in Central Europe having received the SET mark for its Merchant module in October, 1999. In September 2000 the company and its "Java Merchant with SET" product was chosen (with IBM, Globeset and Brokat) to become an Approved SET Test Partner.

### 13.2.6 Firewalls

Major organizations in telecommunications, banking and financing, government sectors, multinational lawyers' offices and architect/engineering companies are potential customers for firewalls. The market leader in firewall software is Check Point Software Technologies (Israel), other major vendors are: Axent Technologies (U.S.) with "Raptor", Network Associates (U.S.) with "Gauntlet", "McAfee Firewall" and "PGP Personal Firewall" , Cyber Guard (U.S.), Sun (U.S) with "SunScreen". Novell is also present in the market with its "Border Manager". There are some free firewall software in use that can be freely downloaded such under GNU public license

such as LINUX. Smaller companies with less resources prefer the solution of a router with built-in packet filtering ( i.e. “Pix” of Cisco) Personal security appliances costing less than $ 100 might be a best prospect for small companies.

### 13.2.7 Virtual Private Networks (VPN)

International companies with several sites operating in Hungary are the main customers of VPNs using two solutions; either a firewall software with a VPN option i.e. VPN-1 of Check Point (Israel) or using a router (Cisco with IPSec technology or Nortel). Practically all firewall software vendors mentioned above offer VPN solutions. “PGP VPN” of Network Associates has a market here for intranets. MATAV, the Hungarian Telecommunications company, has built a nationwide network using SUN servers, Cisco routers, and Belle management software offering VPNs to companies with several sites or Internet Service Providers. Pantel, an alternative ISP to MATAV, also offers VPN services.

### 13.2.8 Intrusion detection and monitoring

The market leader is the U.S. Internet Security System (ISS) having a Hungarian distributor (Noreg Kft). Compaq and Bull selling their own ISS products based on their worldwide agreement are also major players in the market. Other main suppliers are Axent Technologies (bought by Symantec, U.S.), Network Associates (U.S.) with “Cyber Cop” and “PGP Personal Intrusion Detection.” Monitoring is handled by the various modules of the administration tools (i.e.”Open View” of HP, “Tivoli” of IBM etc.)

### 13.2.9 Knowledge Management

Knowledge management is used mainly with large international companies but not involving the field of security issues. Internet Security System has its “SafeSuit Decision” implemented with MATAV, the Hungarian Telecommunications company; it is the only one application in Hungary. MATAV was the first company in Central-Europe to buy the ISS modules. A pilot project was completed in October 2000, and during 2001 ISS will be introduced to the whole system of MATAV, including 10, 000 PCs and a large number of servers. Noreg Co.Ltd, an ISS solution Partner, has represented ISS in Hungary since 1997. Noreg is specializing in data security risk audit and intrusion detection.

### 13.2.10Encryption

There are no legislative barriers preventing the sale of encryption software in Hungary. The market leader in encryption software is “PGP” of Network Associates (U.S.). Other major vendors present in Hungary are: RSA Laboratories (U.S.), Entrust Technologies (Canada), Secude (Germany). In the field of cryptographic accelerator and key management devices the following suppliers are trying to penetrate the market: IBM, Chrysalis ITS (Canada), nCypher (U.K.- with two instances of use in Hungary), Algorithmic Research (Israel), Rainbow Technologies (U.S.) and Compaq.

### 13.2.11 Smart Cards

The use of smart cards is not yet widespread in internet security, although smart card technology is used with student IDs and the phone cards of MATAV. The main suppliers are all present in Hungary; Active Card (France), GEMPLUS (France), Bull (France) Schlumberger (France) and Oberthure Card System (France). The French suppliers dominate the market, the only U.S. smart card manufacturer known to explore the Hungarian market is Spyrus. K& H Bank started a test run of e banking in November of 2000 for 5,000 selected retail clients in cooperation with MATAV and its Internet Service Provider, MatavNet Co.Ltd. using smart-card client identification, PKI authentication and digital signatures.

### 13.2.12 Content Screening

Market leaders are: Content Technologies (U.K. bought by Baltimore, Ireland) with "Mime Sweeper" and Secure Computing (U.S.) with its "Smart Filter" product and e-Safe (U.S.) with "Aladdin". Major system integrators (Compaq, Montana, ICON) market these products.

### 13.2.13 Antivirus

Since the appearance of the e-mail viruses, virus alertness is more intensive in Hungary . Market leaders are the products of the U.S. Norton, McAfee and "Innoculen" of Computer Associates. The antivirus programs (F-Secure and F-Prot) of Data Fellows (Finland) compete with the U.S. products. VirusBuster Hungary Ltd. established in 1989 provides virus protection services representing Sybari (U.S.) and Sophos (U.K.) but has developed its own virus-scanning engine.

### 13.2.14 Security assessment tools

Internet Security Systems (ISS) is the market leader in this field too, closely followed by Axent Technologies (U.S.) and Network Associates having about an equal market share.

### 13.2.15 Enterprise security

Major vendors of enterprise security products are all represented in the market (Axent Technologies with "Enterprise Security Manager", "Secure ID" and "Keon, RSA Laboratories with "ACC", Entrust Technologies (Canada) and Novell. However, no significant sales are expected in the near future.

### 13.2.16 Market opportunities

Security will be more and more in the focus with banks, financial institutions, major industrial companies, portals and e-marketplaces. Best prospects are: single sign-on authentication/authorization, PKI, firewall security appliances for personal use, content screening, and anti-virus products. However the main obstacles to sales will be slow evolution of Hungarian law and the low level of Internet penetration in

Hungary. Furthermore, IT managers of the companies who would understand security issues have no power to decide on purchases, rather it is the decision of top management. The key issue is to make top decision-makers aware of security threats and the importance of purchasing security products.

A consortium made up of MATAV (Hungarian Telecommunications Co.), OTP (the Hungarian National Savings Bank), Andersen Consulting and Compaq Computer Hungary Co. Ltd. established Hungary's first B2B electronic marketplace (technology supplied by the U.S. company, Commerce One) in September of 2000. The test will run until April 2001 but currently 300 companies have already registered. According to Compaq's estimations, in 4-5 years time 30 percent of all indirect (products not directly related to manufacturing) procurement will be transacted electronically amounting to HUF 150 billion ($ 535 million). In October 2000, Hewlett-Packard, Oracle and PricewaterhouseCoopers established a horizontal marketplace called "First Hungarian E-Market Co.Ltd" for the sale of IT and office equipment and services. The founders expect to have $ 100 million turnover already in the first year. Further foreign investors are planned to be involved in the venture. In November 2000, PricewaterhouseCoopers (PWC) started the test run of a vertical e-marketplace of pharmaceuticals called PharmaLink.

The IT Government Commissioner's Office is working on the Hungarian government's electronic public procurement system planned to start operation by January 31, 2002.

### 13.2.17 Legal framework

The draft law on electronic signature was accepted by the Hungarian executive branch of government on February 21, 2001 and was sent to Parliament to be discussed It is expected that the Parliament will pass the law by the end of June 2001. Since Hungary anticipates being a member of the European Union around 2004, the GoH closely follows EU directives when drafting new legislation. The new law aims to determine:

- the legal effects of digital signatures and electronic documents
- requirements for Certification Authorities (CA) and certified CAs and the terms and conditions regulating their operation in the Hungarian market
- supervision system of Certification Authorities

The digital signature law will not regulate encryption of documents. Therefore until there is a separate law on encryption, it should be ensured in the digital signature law that key-pairs used for creating digital signature should not be used to encrypt documents, although national security agencies reserve the ability to decrypt documents.

The Inter-Ministerial Committee on Information Technology of the Prime Minister's Office has issued proposals on how to regulate IT security based on the recommendations of Trusted Computing Security (Orange Book), ITSEC, Common Criteria and CRAMM (CCTA risk analysis and management methods).

## 13.3 Competitive analysis

Even though there are no official statistics, market players estimate that U.S. products have about a 70-80 percent market share of the internet security market. There is practically no Hungarian domestic competition except for the few examples mentioned about PKI and authentication. Third country competitors include: Check Point Software Technologies (Israel), Active Card (France), Baltimore (Ireland), Entrust (Canada), Sonera Smart Trust (Finland), Brokat (Germany, Secude (Germany), Chrysalis ITS (Canada), nCypher (U.K.). Key competitive factors are price and the reliability of the products.

Local analysts posit that U. S. products seem to be expensive. Moreover, they caution that U.S. companies should be flexible and not use their global price list in Hungary. Some American companies wanting to penetrate this market have already utilized this strategy and feel that it has resulted in higher sales. U.S. companies are recommended by local consultants to establish either a representation office or a Hungarian subsidiary to coordinate sales. Indirect sales through a Hungarian partner, a value-added-reseller or a system integrator, are held to be even more efficient by some quarters.

## 13.4 Statistical information

The estimated number of regular Internet users in Hungary is between 600,000 to 800,000 people. (Total population in Hungary is: 10,000 million people.) According to a survey conducted by Carnation Internet Consulting in October 1999; 360,000 people have internet access from schools, 236,000 are corporate and governmental users, and 221,000 are home and small-office users (with an overlap of 104,000 this totals to 713,000 users). According to Andersen Consulting the number of Hungarian households with computers are between 300,000 to 350,000, but just a low percentage of them (25%) is equipped with Internet access technology. While the number of private internet subscribers is expected to grow by 50-70%, the number of business users doubles yearly. Analysts of Concorde Securities Rt. estimate that 7 percent internet penetration is expected to grow to 9 percent in 2003 and 12.5 percent in 2005. According to a more optimistic version this rate can reach 30 percent and 50 percent respectively in the same timeframe.

Sixty-five percent of small and 75% of medium-size companies are estimated to have used the Internet in 2000. Internet usage with large companies amounts to 95%. There is a relatively low number of Intranets in the business sector. Just every third of the largest companies, about 18% of the medium-size organisations and 4-5% of small businesses established their own network. The same trend is noticeable in the spread of extranets, however, the penetration is lower. About one-third of the large organisations have web-sites, but this ratio is lower as the company size decreases. Currently a low percentage of the organisations conduct e-business, but it is expected to increase significantly due to emerging market needs.

Taylor Nelson Sofres Modus research shows, organisations having Internet access use the service for mainly e-mailing, web-browsing, gathering financial, economic market information and communicating with their clients through the company's homepage.

About thirty Internet Service Providers (ISPs) provide access services to the approximately 120,000 dial-up subscribers and to corporate accounts through VSAT, ISDN or managed leased lines. Three major ISPs (MATAVNet, PSINet Elender, and GTS Datanet) cover 85 % of the market. Two of these have US interest. PSINet acquired Elender (30 % market share) in September 1999. GTS, a US based alternative telecommunications service provider owns Datanet (15 % market share). A new entrant into the Hungarian ISP market is UUNet (member of the WorldCom Group) which started Internet services in early August 2000.

### 13.4.1 Business-to-Consumer (B2C) E-commerce

There are currently about 200 Hungarian companies selling their products over the Internet. In 1999, the estimated size of this type of commerce was HUF 209 million (USD 774,000) or less than one percent of total retail sales. In a few years time, the largest twenty virtual shops are expected to account for the majority of the turnover. Business-to-consumer transactions are estimated to amount to HUF 1 billion ($ 3.5 million) in 2000 and will reach HUF 560 billion ($ 2 billion) in 2010. The relatively slow increase of B2C e- commerce is due to three factors: low Internet penetration, few opportunities of online banking (that would change soon) and the lack of efficiently organized home delivery.

### 13.4.2 Product profiles on business-to-consumer e-commerce Webster:

| | |
|---|---|
| Books, CD-ROMs | 25.64% |
| Music | 15.38% |
| Stock trading | 12.82% |
| Stationery | 10.26% |
| Electronics, HW | 7.69% |
| Gifts | 7.69% |
| Others | 20.51% |

Over 85% of B2C purchases are transacted with payment collected on delivery.

The above figures do not include B2C financial services. Out of 38 banks, 13 have a Website and four provide banking services on the Internet. Hungary's ten biggest banks plan to launch Internet banking services within two years.

### 13.4.3 Business-to-Business (B2B) E-commerce

According to a survey by Carnation Strategic Internet consulting, B2B e-commerce was transacted until 2000 almost exclusively through Electronic Data Interchange (EDI) systems. EDI was introduced in Hungary in 1996, by the end of 1999 there were 400 users, and in 2002 the number of EDI applications may reach 1,500. These are mainly in the retail, automotive, and Fast Moving Consumer Goods sectors. It is

expected that over the next three years, Internet based solutions (WEB-EDI and internet/EDI systems) will obtain a larger share of B2B transactions.

Business-to-Business e-commerce in Hungary (in HUF millions)
1 USD=280 HUF in 2000

Carnation estimates that B2B e-commerce amounted to $ 11 million in 2000 and is expected to reach $ 53 million in 2001 and $ 303 million in 2002.

### 13.5 Contact information

Prime Minister's Office
IT Government Commissioner's Office
Mr. Zoltan Sik, Government Commissioner
Szilagyi Erzsebet fasor 11/b.
H-1024 Budapest
Tel: (36-1) 315 2550 Fax: (36-1) 315-2536
e-mail: sikz@ikb.meh.hu
www.meh.hu

Compaq Computer Hungary Ltd.
Mr. Gyorgy Beck, Managing Director
Central and Eastern Europe
Nemetvolgyi ut 97.
H-1124 Budapest
Tel: (36-1) 458-5555 Fax: (36-1) 458-5515
e-mail: gyorgy.beck@compaq.com
www.compaq.hu

Synergon Rt.
Mr. Tibor Gyuros, CEO
Mr. Levente Zsolt Palfy, Consultant
IT Security and System Management Division
Baross u. 91-95.
H-1047 Budapest
Tel: (36-1) 399 5500 Fax: (36-1) 399-5599
e-mail: gyuros.tibor@synergon.hu
e-mail: palfy.zsolt.levente@synergon.hu
www.synergon.hu

Montana Rt.
Mr. Tamas Kovacs, Information Security Director
Gyulai Pal u. 13.
H-1085 Budapest
Tel: (36-1) 327-9800 or 327-9833 (direct)
Fax: (36-1) 327-9801
e-mail: tom@montana.hu
www.montana.hu

debis IT Services Dataware
Dr. Akos Simonyi, Managing Director
Mr. Peter Gyure, Director Developments
Angol u. 34.
H-1149 Budapest
Tel: (36-1) 467-1100  Fax: (36-1) 251-5517
Peter.gyure@dataware.debis.hu

Noreg Kft.
Dr. Zsolt Koros, Managing Director
Varsanyi I. u. 26-34.
H-1027 Budapest
Tel: (36-1) 488-0427  Fax: (36-1) 212-8401
e-mail: zsolt.koros@noreg.hu
www.noreg.hu

PricewaterhouseCoopers Management Consulting Services
Mr. Zoltan Patocs, Consultant
PwC DYNASoft Rt.
Wesselenyi u. 16.
H-1077 Budapest
Tel: (36-1-) 461-9100  Fax: (36-1) 461-8800
e-mail: zoltan.patocs@hu.pwcglobal.com

ICON Kft.
Mr. Marton Salamon, Managing Director
Tuzer u. 39-41.
H-1134 Budapest
Tel: (326-1) 452-1250  Fax: 936-1) 452-1251
e-mail: msalamon@icon.hu
www.icon.hu

Sun Microsystems Hungary Ltd.

Mr. Janos Keresztesi, Managing Director
Mr. Tamas Zsemlye, Systems Analyst
Kapas u. 1015.
H-1027 Budapest
Tel: (36-1) 489-8900  Fax: (36-1) 201-2731
e-mail: janos. Keresztesi@hungary.sun.com
e-mail: tamas.zsemlye@hungary.sun.com

ProWare, The Business Security Company
Mr. Adam Tresch, PKI consultant
Koszeg u. 27.
H-1144 Budapest
Tel: (36-1) 273-2678  Fax: (36-1) 273-2667
e-mail:  tresch.adam@proware.hu

Pik-SYS Servicing and consulting Ltd.

Mrs. Maria Pistar, Managing Director
Szentmiklosi ut 18.
H-1213 Budapest
Tel: (36-1) 455-6000 Fax: (36-1) 455-6005
e-mail: info@piksys.hu
www.piksys.hu
(antivirus software, data encryption, firewalls, intrusion detection)

Guardware Co.Ltd.
Dr. Istvan Kerese, Managing Director
Ulloi u. 102.
H-1089 Budapest
Tel: (36-1) 459-1780 Fax: (36-1) 459-1799
e-mail: kerese@guardwaresystems.com
www.guardwaresystems.com

Carnation Strategic Internet Consulting
Ms Olga Lipkovics, CEO
Orbanhegyi ut 5.
H-1126 Budapest
Tel: (36-1) 489-9000 Fax: (36-1) 393-5000
e-mail: lipkovics@carnationresearch.hu
www.carnationresearch.hu

VirusBuster Hungary Ltd.
Mr. Peter Agocs, Director Development
Kalaszi u. 11.
H-1031 Budapest
Tel: (36-1) 430-8350 Fax: (36-1) 430 8354
e-mail: pagocs@vbuster.hu
www.vbuster.hu

# 14 Ireland

# 15 Italy

## 15.1 Summary

The Italian information and communication technology (ICT) market is still lagging behind other European countries, but it is rapidly catching up, with Italian companies increasingly investing in ICT technologies.

The Italian market for Internet and related services boomed in 1999, and both Business-to-Business and Business-to-Consumer e-commerce applications took off. E-commerce is expected to become one of the most dynamic and fastest growing segments in the next three years, thanks to improved access infrastructure and to new Italian government plans for accelerating ICT acceptance and e-commerce adoption.

The "culture" of ICT and Internet security in Italy is still at an embryonic level, but is it expected to develop rapidly. There is still significant resistance at the managerial

level to approve specific investments for ICT and Internet security plans, but the situation is changing rapidly. Companies are increasingly relying on intrusion detection systems, more secure networking equipment, firewall software and equipment, secure content control software, internet access control tools, and security authentication, authorization and administration tools. Security management policies and management support applications are also being widely implemented.

The need for specialized skills to implement internet security strategies is leading Italian companies to depend on external consulting, and excellent opportunities exist for American service providers offering the strategy, marketing, design, and technical products and services associated with building a secure internet environment.

The domestic market relies heavily on the expertise of foreign companies, and U.S. firms account for 80 percent of the revenues of foreign-owned establishments in Italy. As U.S. technological expertise is highly regarded, and U.S. advancements in the internet security sector are widely recognized, excellent opportunities exist for specialized U.S. computer services companies. The greatest opportunities for success are for American companies offering innovative and sophisticated services, and willing to team up in cooperative agreements with well-established local firms.

Sources utilized: No official statistics are available in Italy on the Internet and e-business/e-commerce applications. The estimates and forecasts indicated are based on interviews, information from trade sources, and reports from the trade associations ASSINFORM, ASSINTEL, and EITO, and from the market research organizations Net Consulting, Gartner Group, Databank Consulting, IDC, SIRMI, and Osservatorio Bocconi.

## 15.2 Market Profile

### 15.2.1 The Internet Security Market

Italy is the world's sixth largest industrialized economy and Europe's fourth largest market for the information and communications technology (ICT) industry. Although some structural problems still hinder the full evolution of the Italian ICT market, the growth of the ICT sector is accelerating, following the pattern of other countries in Western Europe. Italian companies are increasingly investing in ICT solutions as a means to implement renewed business strategies and face the challenges of the new Web Economy.

The total Italian market for information technology in 1999 reached sales of $17.9 billion, a 10.6 percent increase over 1998, while sales in the telecommunications sector - including equipment and services -were more than $ 34.8 billion, a 14.6 percent increase over 1998. It is estimated that in the year 2000 ICT market revenues totaled $ 59 billion, a growth of 12.5 percent.

The "culture" of ICT and Internet security in Italy is still at an embryonic level, but is it expected to develop rapidly. Many Italian companies still lack a systematic approach to security issues in terms of prevention, identification and monitoring the existing security measures. There is still a significant resistance at the managerial

level to approve specific investments for ICT and Internet security plans, especially if the company has not suffered from, or has not become aware of, direct security attacks. In many companies the top management has started to develop some security awareness and to perceive security as a core business requirement, but only after the latest worldwide cyber attacks and e-mail diffusion of viruses were widely publicized. Security, however, becomes one of the major concerns of Italian companies and consumers when it comes to e-commerce transactions and possible payment fraud.

According to the 2nd Report on ICT Crimes from the Italian Sicurforum Association, a sample of 200 Italian companies and public organizations in 1999 revealed number of attacks to ICT systems grew by 242 percent from 1998. Virus attacks represented 32.8 percent of the total, followed by theft of machines with data (15.6 percent), unauthorized data access (11.6 percent), unauthorized use (11.6 percent), unauthorized changes (8.9 percent), unauthorized access to telecom services (8.6 percent), and denial of service attacks (8.3 percent). Two thirds of the attacks were attributed to external sources, and the remaining third to internal staff. The number of attacks is projected to increase as internet usage develops.

No specific statistics are available on the Italian Internet security market, but trade sources estimate that Internet related expenditures to support intranet/extranet and electronic commerce solutions in Italy were $ 1.6 billion in 1999 and reached $ 2.7 billion in the year 2000.

The diffusion of IP based network platforms is fueling an increased demand for internet security services and solutions from Italian companies. A growing number of large and medium sized Italian businesses are investing heavily in Intranet/Extranet infrastructure and are implementing web sales and purchasing applications to meet their needs for improved interaction with suppliers and customers. All major industrial groups are also organizing for e-procurement. Companies are increasingly resorting to intrusion detection systems, more secure networking equipment, firewall software and equipment, secure content control software (anti-virus and malicious code detection), internet access control tools, and security authentication, authorization and administration tools. Security management policies and management support applications are also being widely implemented. The adoption of Virtual Private Networks is still at an early stage, and the use of biometrics has not started yet.

Telecom security will represent a special market driver, as a result of the extraordinary development of the Italian telecom infrastructure market and of the increased demand for network management systems. Telecom security encompasses software solutions that allow network monitoring and fraud detection. IDC estimates that telecom security expenditures in Italy grew from $ 2.5 million in 1998, to $ 7.5 in 1999, to $ 11.3 in the year 2000. They are expected to reach $ 15 million in 2001, $ 19.3 million in 2002, $ 21.7 million in 2003, and $ 24.3 million in 2004.

Another major market driver for the internet security sector will be increased investments of the Italian government in ICT technologies, and the related demand for security technologies, especially certification authority services and digital signature related services. The Italian government within the framework of the European Union’s E-Europe program has recently approved an important e-government action

plan, calling for an investment of $1.3 billion. It aims to offer higher levels of efficiency, integrated and higher quality public services, and Internet access to information and services for all citizens. Among the actions being taken are the creation of a nation-wide extranet, which will connect and integrate all central and local government networks; the creation of specific portals for accessing different government services; issuance of one million electronic ID cards/smart cards to allow easier access to public services; adoption of e-procurement at the central and local government levels; and countrywide promotion and use of digital signatures.

These actions will be made possible by the final implementation of the so-called "Bassanini" law of 1997 and subsequent related decrees and notes, that recognize and set the standards for the legal validity of digital contracts and digital signatures based on the public key infrastructure system. Digital signatures will be utilized as an important support tool to simplify bureaucratic procedures, and their extended use is expected to reinforce the level of trust in e-commerce transactions and to accelerate the diffusion of e-business in the Italian economy.

Internet security products and solutions will also be in high demand in on-line banking and on-line trading of financial services. Banks are investing considerable resources in e-commerce applications both to sell their own home and corporate banking services, and to support the e-business strategies of their clients by developing virtual malls and portals and by supporting secure transactions. The on-line trading market took off in 1999, totaling 4 percent of all traded securities, a share that is forecast to increase to 20 or 30 percent in the next two to three years. It is expected that the number of clients utilizing on-line trading services will grow from 200,000 in the year 2000, to 450,000 in 2001, and to 700,000 in 2002. Total investments in stocks and bonds are expected to increase from $4 million in the year 2000, to $11.5 million in 2001 and to $19 million in 2002. The possibility of accessing financial markets through new generation cellular phones will contribute greatly to the development of this market, and demand for specially developed smart cards should increase.

As the use of the internet becomes pervasive, the Internet security market will develop immensely, and will offer excellent opportunities to American companies providing innovative security solutions and services.

The growing complexity of technologies is leading Italian companies to depend increasingly on external service providers to supplement their in-house capabilities, and to operate efficiently and cost-effectively. It is expected that U.S. firms will play a key role in providing the strategy, marketing, design, and technical products and services associated with building a secure internet environment in Italy.

### 15.2.2 Internet Penetration

After a slow start, since 1999 Internet usage is experiencing explosive growth. The number of business and domestic Internet users is booming: Internet users were estimated at approximately 12 million at the end of 2000, projected to reach 29 million by 2003. This growth is pushed by the availability of improved access infrastructure, new subscription options, free Internet access and new Italian government plans for accelerating ICT acceptance and e-commerce adoption.

According to recent surveys, 1.5 million Italian businesses were connected to the Internet at the end of the year 2000 -- out of a total of 3.4 million - and 300,000 of them had a web site. Connected companies are expected to surpass 2 million by the end of 2001, and to become the totality by the year 2003. Many small and medium sized enterprises are less inclined to innovate and have yet to invest in the Net.

In the consumer segment, Internet subscriptions grew from 540,000 in 1998 to over 3.7 million in 1999, and to an estimated 4.5 million in the year 2000. Sales of PCs for home use are expanding and approximately 32.5 percent of Italian households now have one. Mobile phone diffusion in Italy is among the highest in the world, and the Internet consumer market will be driven by the availability of web-enabled new-generation mobile phones.

### 15.2.3 E-Commerce

The total market value for e-commerce transactions in Italy was estimated at over $1.1 billion in 1999 and at $4.3 billion in the year 2000. It is projected to register revenues of close to $8 billion in 2001 and to reach over $ 50 billion by 2003. According to IDC, Web buyers are projected to increase from 960,000 in 1999 to 9.8 million in 2003.

B2B e-commerce transactions passed from an estimated $ 970 million in 1999 to $ 4 billion in the year 2000, while B2C transactions went from $195 million in 1999 to $350 million in 2000. They are expected to reach respectively $7 billion and $ 890 million in 2001, and $ 38.5 billion and $ 11.5 billion in 2003, with the relative weight of B2B transactions growing constantly.

The main factors fueling the development of e-commerce in Italy are expected to be:

1) increasing recognition of e-commerce as a means to provide better support to customers and suppliers;
2) improved consumer protection legislation;
3) Italian government legislation that recognizes the legal validity of digital signatures and digital contracts;
4) agreements between Italian banks and credit card operators to introduce Secure Electronic Transaction (SET) protocol;
5) Italian government programs to accelerate the development of a new economy culture, and initiatives of trade associations, major organizations and local governments to foster innovation and to promote e-commerce, especially among small-and medium-sized enterprises;
6) mobile phone diffusion among the highest in the world, which will enable both the business and consumer segments to take advantage of new technologies for e-commerce transactions.

### 15.2.4 Italian Legislation Related To Internet Security

Italian legislation is basically in-line with EU directives, although several aspects are still considered "gray areas" and will be solved as the situation evolves.

As mentioned, Italian legislation recognizes the legal validity of digital signatures and digital contracts through the so-called "Bassanini" law and subsequent related decrees and notes. This set of laws and decrees establishes the criteria and methodology for the development, filing, transmission, duplication, reproduction and validation of electronic documents. AIPA, the Information Technology Authority for the Public Administration, will maintain a list of Certification Authorities, which can be public or private organizations meeting specific reliability requirements. To date, AIPA has granted certification authority to the following eight companies: SIA - Societa' Interbancaria per l'Automazione/Cedborsa, SSB-Societa' per i Servizi Bancari, BNL Multiservizi, InfoCamere, Finital, Saritel, Postecom and Seceti. These companies have joined into the trade association Assocertificatori.

Italian legislation fully complies with EU consumer protection directives with regard to the specific information an e-commerce site must provide, and sets rigid privacy protection requirements for the opening of an e-commerce site. The Legislative Decree on Commerce of March 1998 improves consumer protection and identifies the responsibilities of internet service providers, system operators, and content providers. A special committee of the Italian Ministry of Industry is presently in charge of certifying electronic commerce sites.

#### 15.2.5 Best Sales Prospects

Intrusion detection systems, secure networking equipment, firewall software and equipment, secure content control software (anti-virus and malicious code detection), security authentication, authorization and administration, PKI/CA, security monitoring and management services.

The development of e-business in Italy will create superb opportunities for companies specializing in Internet security. Consulting services to assist the customer in developing risk analysis and assessment and security management are expected to grow in the next two years. Forecasts indicate that outsourcing services will represent one of the fastest growing market segments.

## 15.3 Competitive Analysis

#### 15.3.1 Market position of locally-owned establishments

The trade association Federcomin and the market research company Net Consulting estimate that the number of Italian companies active in the Internet economy grew from approximately 3,330 in 1999 to more than 4,800 in the year 2000. Although no statistics exist for the Internet security market, trade sources estimate that locally owned companies hold approximately 40 percent of the Internet security market.

Some of the most important Italian companies offering internet security products and solutions include:

- Telecom Italia, the most important telephone operator which also offers internet access and e-commerce services;
- I.Net, exclusively oriented to the business market, controlled by the information services company Etnoteam and by British Telecom;

- IT.Net, specialized in Internet access and services to the business market, recently acquired by the fixed and mobile telecom operator Wind.

Several new telecom operators offering Internet access also provide internet security related services directly. Among the most important are 1)Albacom, a joint venture between the Italian bank Banca Nazionale del Lavoro (BNL), British Telecom, the giant oil and gas conglomerate ENI, and the Italian entertainment conglomerate Mediaset; 2) Wind, a partner of Nokia and the on-line bank ImiWebTrader to provide Italy's first on-line trading service from WAP phones; and 3) Infostrada, previously owned by Olivetti/Mannesman and then by Vodafone, and recently acquired by Wind.

All the most important Italian software and service companies offer security related products and services. They include: Gruppo Finsiel, the large software and services group controlled by Telecom Italia; Elsag (part of the Finmeccanica group); Datamat Ingegneria dei Sistemi; Gruppo Formula; Etnoteam, which controls the ISP I.Net; Engiweb.com of Gruppo Engineering; Intesis of the Finmatica Group; Mover, Siosistemi, Zucchetti, and several others.

### 15.3.2 Third Country Competitors

Internet security products and services offered by foreign-owned establishments represent about 60 percent of the total Italian market.

The importance of foreign companies in this sector is forecast to remain high in the next three years. Many foreign computer hardware and software vendors and service companies are already present in the Italian market through subsidiaries. They include the French companies Bull, Atos, Sema, and GFI, the German firm SAP and Siemens, the Belgian Ubizen, the British Marconi, and the Spanish Panda Software.

### 15.3.3 U.S. Market Position

U.S. companies dominate the Internet security market, and they are estimated to hold approximately 80 percent of the import market.

All the leading U.S. information and communications technology firms - Cisco Systems, Compaq, Computer Associates, Hewlett Packard, IBM, iPlanet, Lucent Technologies, Microsoft, Novell,, 3COM, etc. - are directly present in Italy through subsidiaries or branch offices. Specialized companies such as BMC Software, Check Point Software Technologies, ISS-Internet Security Systems, Network Associates, RSA Security, Symantec, and Verisign also have subsidiaries in Italy, and others such as Cyber IQ Systems, Entrust Technologies, and Rainbow Technologies are represented through Italian companies.

Several U.S. consulting and services companies are already strongly positioned in the Italian market. They include the EDS group; Accenture; GE Information Services; Cap Gemini Ernst & Young; KPMG; and Price Waterhouse Coopers.

Good opportunities exist for other highly specialized U.S. computer services companies with specific vertical market experience. They should be willing to partner

with well-established Italian firms for cooperative agreements. As U.S. technological expertise is highly regarded, and U.S. advancements in the Internet security sector are also widely recognized, the United States is expected to increase its already excellent market position over the next three years.

### 15.3.4 Competitive Factors

Solid financial and organizational structure, a high degree of professionalism, proven knowledge of innovative technologies, business reputation, and business references are key factors for a supplier's success in Italy. Availability and integration of high-quality solutions, adherence to industry standards, vertical market experience, reliable pre-sales and after-sales service, training and timely delivery have also become crucial to ensuring customer satisfaction.

A crucial factor for new-to-market U.S. firms is to understand the structure of the Italian market and the user culture, and to communicate constantly with clients. It is essential for suppliers to understand and analyze customer needs fully and possess the necessary skills and flexibility to offer new value-added, integrated solutions.

### 15.3.5 End-User Analysis

The telecom sector is one of the most important end-users for Internet security solutions and products. The arrival in Italy of new telecom service providers and the rapid growth of the Internet are resulting in major investments to upgrade and expand telecommunications infrastructure and to guarantee telecom security.

The manufacturing sector is also an excellent end-user. Larger companies are investing in Intranet/Extranet and e-business projects and require the assistance of specialized consulting firms that can supplement their own internal resources.

The banking/financing and insurance sectors have started to invest in Internet solutions and e-commerce projects. As applications such as home banking and on-line financial and insurance services develop, Internet- and Intranet-related computer and network services are expected to be in great demand. Information technology and telecommunications will continue to play a key role in supporting the strategies of banks, financial institutions, and insurance companies to improve productivity and profitability.

The public administration sector (at both the national and local government levels) is also an important prospective client for the services market. As mentioned, the need for higher levels of efficiency and to offer higher quality public services will play a key role in the growth of PKI/CA. Significant developments are expected in the fields of e-procurement, health care management and fiscal services.

15.3.6 Market Access

*15.3.6.1 Import Climate*

The Italian climate for cooperative agreements and investment from U.S. companies is favorable. There are no trade barriers limiting the presence of foreign computer services companies in Italy. In fact, many multinational companies have established an office in Italy. In some cases, foreign computer services companies, usually specialized in vertical market niches, have reached agreements with well-established local companies or major end-users and have relocated personnel to Italy.

ISO-9000 certification for quality assurance is not mandatory in Italy. However, major Italian clients increasingly require that their suppliers be certified as a prerequisite for doing business with them. The Italian institute IMQ (Istituto Italiano Marchio Qualita'), which is part of EQNet (European Quality Systems Assessment and Certification Network), is the official local certifying agency for ISO-9000 in the information technology and software sectors.

*15.3.6.2 Distribution/Business Practices*

Major multinationals and large companies use their own direct networks and sales organizations. U.S. firms with no direct presence in Italy usually operate through locally appointed partners. These are well established throughout the country, offer good pre-sales assistance and after-sales technical services, have experience in the different market sectors, and maintain person-to-person contact with customers. American companies interested in entering the Italian market should consider cooperative arrangements or joint ventures with carefully selected Italian partners.

*15.3.6.3 Financing*

Financing practices in this sector adhere to normal business and banking standards, with the majority of the transactions arranged through private agreements and banking institutions. U.S. companies should be aware that the turnaround time for paying invoices is almost always 90 days in Italy, but in many cases it may be as many as 120-180 days. The Italian public sector is very slow in paying its debts, sometimes taking more than a year. A certain degree of flexibility is considered normal in the establishment of terms and conditions.

*15.3.6.4 Trade Promotion Opportunities*

**15.4 SMAU**

The most important Italian information technology and telecommunications show. Held in Milan every year in October. Next edition: October 18-22, 2001. Over 3,000 exhibitors, of which 1,100 represented foreign companies - 500,000 visitors. Organizer: SMAU-COMUFFICIO, Attn. Ms. Maura Gritti, International Marketing Manager - Via Merano 18, 20127 Milano - Tel. 39/02/28313-251, fax 39/02/28313-470, maura.gritti@smau.it, www.smau.it

For the eighth consecutive year, the Commercial Service of the U.S. Department of Commerce in Italy will organize a U.S. Pavilion at the SMAU show. For further information please contact:

### 15.5 U.S. DEPARTMENT OF COMMERCE SERVICES

Commercial Service
Attn. Ms. Maria Andrews, Principal Commercial Officer
Via Principe Amedeo 2
20121 Milan, Italy
Tel. 39/2/6592260 Fax 39/2/6596561
www.usatrade.gov
Milan Office Box@mail.doc.gov

U.S. Department of Commerce
The offices of the Commercial Service in Italy offer U.S. companies the Gold Key Service, a program tailored to the needs of business executives travelling to Italy and looking for distributors or partners. The CS staff identifies, selects, and sets up appointments with Italian key contacts in the specific sector of interest. For information, please contact:

American Embassy Rome
Commercial Service
Via Vittorio Veneto 119/A
00187 Roma
Tel. 39/06/4674-2382
Fax. 39/06/4674-2113

The U.S. Department of Commerce in Washington organizes several trade missions and "Matchmaker" delegations to Europe and Italy. For information about upcoming events, please contact:

Ms. Molly Costa
Matchmaker Product Manager
U.S DEPARTMENT OF COMMERCE
US&FCS/HQ/EPS/MM
14th and Constitution Ave., NW
Washington, DC 20230
Tel. (202) 482-0692 Fax (202) 482-0178

The U.S. Department of Commerce also offers other services aimed at assisting American companies wishing to export. For further information, contact the nearest U.S. Export Assistance Center.

# 16 Luxembourg

# 17 The Netherlands

## 17.1 Summary

The Internet Security Products and Services market offers one of the fastest growing Information Technology (IT) sub-markets in the Netherlands. With the rapid increase in electronic communications and use of the Internet, the past few years have seen much progress in both a growing awareness of the need to protect computers, networks and computer data, as well as in new technologies that can offer increased security and protection. This report highlights the computer hardware/software solutions and services side of the market for Internet security products, an area in which U.S. companies have taken a lead and that offers good prospects for future increased U.S. exports.

Trade sources estimate the security products portion of the Dutch IT market at about $ 195 million in 2000. This market segment is expected to grow by about 10-15 % annually during the next two or three years. The Dutch market for Internet security products and services primarily depends on imports. There is no significant local production and limited exports. The United States, in particular, and European manufacturers are the main suppliers to this market. Demand for Internet security products is strongest from financial organizations; the national government; Dutch multinationals; public utilities; telecommunications and the health care sector. Small and Medium-sized Enterprises (SMEs) are a new and growing segment in the market. Competition in the market is increasing.

While the Dutch ICT market is very competitive with many large players, U.S. companies already active in the Netherlands and those planning to enter the market are expected to benefit from the healthy economic conditions and the growing demand for Internet security products and services. The head start of U.S. exporters in Internet related products and services offers numerous opportunities for increased sales to the Netherlands.

## 17.2 Market Overview

About the size of the State of Maryland, the Netherlands has a total population of almost 16 million people. There is an active working population of 6.6 million people and there are some 90,000 registered companies with a staff of more than five people. There are 6.5 million Dutch households. The Dutch economy is among the strongest in Europe, and continues to show sustained, albeit slowing GDP growth combined with low unemployment. The Dutch Central Planning Office (CPB) recently released 3% growth forecasts for the economy in 2001 and 2.75% in 2002.

With a healthy and growing economy, the Netherlands market for Information and Communication Technology (ICT) in total amounted to approximately $ 23 billion in 2000. The IT market amounted to $10.8 billion and includes: hardware (54 %), software (17 %), computer services (25%) and supplies (4%.). The total Netherlands telecommunications market amounted to approximately $ 12.3 billion in 2000: 80 % of the market consisted of telecommunications services, while the remaining 20 % can be attributed to telecommunications equipment. According to the 2001

IDC/World Times Information Society Index (ISI), the Netherlands ranks tenth on the list of information economies in the world, and second, behind Taiwan, when the information infrastructure is considered.

Contributing to the growth of the market for Internet security products and services are the ever-increasing dependency on computers and computer networks in general, the rapidly increasing use of the Internet, E-commerce transactions, electronic banking, telecommuting, remote access, and privacy concerns. Corporate espionage, use of automated attack tools, and recent virus attacks, e.g. the "I love you", "Melissa" and "Anna Kournikova" worms, as well as hacking incidents and e-mail problems are generally well publicized and attract much attention. The "I Love You" virus alone reportedly created an estimated $25 million worth of damages to Dutch computers in May 2000. Instances like this show how vulnerable computers are to the growing threat of viruses. They stimulate a more general awareness of the threats and are followed by the implementation of new policies, training and education and increased use of products and services that provide better communication security, reliability of information systems and protection of data. Security products used in the Netherlands today include among others: Internet firewalls, anti virus and authentication/authorization products, Virtual Private Networks (VPNs), Encryption, and Public Key Infrastructure (PKI).

Both the public and the private sectors are introducing initiatives to stimulate further security awareness among Dutch businesses and consumers using the Internet. Among these initiatives are systems that send out virus alerts to government and the public. Although there is no standard at this time, the Public Key Infrastructure system, in which Trusted Third Parties (TTPs) are active to verify reliability of buyers and sellers, is becoming more popular in the Netherlands. Major TTPs in the Netherlands include KPN Telecom and Pink Roccade. The use of VPNs is also on the increase. A six months' pilot project recently began in Delft, the Netherlands with electronic ID cards that make use of biometrics technology to identify people. As the technology is not yet considered stable enough to stand on its own, a PIN code is also being used.

### 17.2.1 Internet Security market.

In a July, 2000 survey of the Dutch business market, 79 % of Dutch companies indicated that they have a formal information security policy in place. Some 39% of the surveyed companies employ an IT security specialist. 62.5 % of the companies indicated they had experienced one or more security problems during the previous 12 moths. The survey, which was held prior to the annual Info Security tradeshow in October 2000, further showed that viruses were the largest problem. 58% of the companies interviewed had suffered damages from the "I love you" virus. The love letter virus not only damaged Small and Medium-sized Enterprises (SMEs), but was destructive throughout the Dutch business world. The number two security problem was penetration by hackers (26%) resulting in data theft and digital vandalism. About 11% indicated Denial of Service (DoS) problems. Smaller companies and start-ups that go on the Internet still lack the necessary security implementation. About 25% of the surveyed companies have not installed an Internet firewall. In December 2000, specialists of Dutch security company Control Risk Management (www.control.nl) reported that, as part of a penetration testing program among 350 large organizations worldwide, they had also successfully penetrated the mainframe systems of major

Dutch multinational companies, banks, insurance companies and the government. Within two days or less, they had either accessed the computers through websites or simple passwords. Primary reasons for the ease with which these computers were accessed were errors in software program design (40%), errors in the software program itself (40%) and improper security implementations (20%.) Control Risk Management expects that the situation in the SME segment is worse, as the larger enterprises tend to have a much larger budget for computer security products and services.

The type of security and protective measures implemented for data networks include passwords, used by almost 100% of Dutch organizations; Internet firewalls are used by about 80 % of organizations, while data encryption is used by 40 %, particularly in the financial services sector.

### 17.2.2 Key-players, including early adopters.

Among the first to adopt security policies and implement security products were large users of all types of ICT equipment. These include the Dutch government, e.g. Defense and Ministry of Finance (Internal Revenue Service), the financial services sector (banks and insurance companies) and health care sector. Large Dutch multinationals companies include Royal Dutch/Shell Group, ING Group, Unilever, Ahold, Philips Electronics, Fortis, Aegon, ABN AMRO Holding, AKZO Nobel, SHV Holdings.

The highest penetration of security products currently is with organizations of more than 200 employees, while the lowest form of protection is among Dutch organizations with 20 or less staff. With an increasing number of SMEs active on the web, however, the SME market segment is rapidly growing too. An important task for computer and network security products vendors in this segment is to increase awareness by educating and counseling their prospective customers regarding the risks and possible solutions to security breaches.
In recent years, both the central, as well as local governments have been investing considerably in information technology. In doing business with the Netherlands government, as a member of the European Union (EU), the EU public procurement legislation requires the Dutch contracting authority to publish major tender notices throughout the European Union. Procurement opportunities that are open to U.S. companies are regularly reported by the Commercial Services of the U.S. Mission to the European Union in Brussels, Belgium, phone 011-32-2-5082746.

Comparing the end-user decision-making process in the Netherlands to that in the United States, U.S. suppliers should take into consideration that the sales cycles for computer and network security products are generally longer than in the states. The use of pilots and demo versions is common in the sales process. However, once a customer is convinced of the value and commits to a certain product or range of products, they tend to be loyal to the products chosen. Important selection criteria to the Dutch buyer of computer products in general are: quality, reliability, flexibility and reputation of the supplier, innovative approach, and cost. Continuous innovation in this fast developing market is a necessity.

17.2.3 Legal framework.

Following European directives, the Dutch government is in the process of implementing laws and regulations concerning the Internet and the use of computers. A new law regarding the protection of personal data aims at providing Dutch citizens more insight in the way their personal data are being used and at protecting their privacy. The law will go into effect in 2001. The law complies with the European Data Protection Directive of October 1995 and replaces the data protection act of 1989. Another new law concerns the protection of consumers who buy from a distance via the Internet, phone, fax and mail. This law went into effect in February, 2001. Additionally, there are proposals regarding electronic signatures and liability of Trusted Third Parties, who assign a unique code to a person and record this in a digital certificate. The proposal for a new law on computer crime prevention is under consideration. Privacy of E-mail will be incorporated in the constitution under privacy of letters.

## 17.3 Competitive analysis

17.3.1 Market accessibility and marketing strategies.

The Netherlands offers an open market, which is accessible and welcomes new investments, both foreign and domestic, and in which American products are highly regarded and well accepted. A modern nation, the Netherlands is strategically located in Europe, bordered by the important hinterland Germany to the East, across the North Sea from the United Kingdom to the West, and Belgium to the South. The Netherlands is a founding member of the European Union, and, although small in size, the country plays an important role in the community at various political and governmental levels. The language spoken in the Netherlands is Dutch. English is widely spoken. About 77 % of the population speak English.

The Netherlands is a technologically advanced country offering an excellent transportation and telecommunications infrastructure. In general, there are few known impediments to the international trade in computer and network security products and services that would prevent U.S companies from successfully doing business in the Netherlands. The Netherlands counts more than 1,600 U.S. companies that are established and doing business in the Netherlands, many of them high technology firms.

Most Internet security products and services are advertised in the traditional media, primarily trade magazines. With the growing use of the Internet to gather and compare information and to order products and services, an important tool in product marketing is a Website. Use of the Dutch language prevails. Distributor or reseller networks are used in the marketing and sales of the products and services. Sales leads are also generated through listing of services in trade directories, direct mail, telemarketing, participation in trade fairs, and through word of mouth. Direct mail and advertising are among the more popular promotional vehicles in the Dutch IT world.

In planning to establish a presence in the Dutch market, the Department of Commerce U.S. Export Assistance Centers can assist with market research studies, trade

missions, trade contact lists, International Partner Searches, and setting up overseas appointments through the Gold-Key Matching Service. The U.S. Export Assistance Centers are located in almost all major cities throughout the United States (www.usatrade.gov.) Information regarding the actual establishment and location of a subsidiary office in the Netherlands may be obtained from the Dutch Ministry of Economic Affairs/Netherlands Foreign Investment Agency - www.nfia.com.

Banking facilities for international transactions in the Netherlands generally meet or exceed U.S. standards. All banks are accustomed to various international banking transactions. More information about banking in the Netherlands can be obtained by contacting The Netherlands Bankers' Association (NVB) in Amsterdam, www.nvb.nl. Payments in the Netherlands are usually agreed on a net 30-day basis. Dutch companies on average pay two to three weeks after the agreed upon term.

VIRA, the Dutch association of some 40 attorneys representing major law firms throughout the Netherlands and specializing in all aspects of informatics law, was established in February of 1995. A listing of VIRA members is available via www.vira.nl.

### 17.3.2 Import Climate

As a member of the European Union (EU), the Netherlands applies the EU common external tariff to goods imported from non-EU countries. No tariffs or import duties are levied on computer software products entering the EU countries from the United States. An import duty of 0-3.5 % is levied on most computer hardware products. A Value Added Tax (VAT) of 19% is assessed on computer hardware and software products based on their Cost, Insurance, Freight (C.I.F.) value plus the import duty at the port of entry. Information about tariffs and duties can be obtained from the Dutch Customs: Belasting Douane, telephone: 011-31-45-5743031, www.belastingdienst.nl. EU regulations regarding encryption apply in the Netherlands and encryption products can be freely imported and used.

### 17.3.3 Domestic vs. Third-Country Players

Domestic production in 1999 amounted to an estimated $ 35 million. This includes primarily embedded security features in custom made applications or standard software packages, e.g. financial and database software products, and professional computer services.

Dutch companies active in the security products and services sector include: Tunix Open Systems a consultant and developer of firewalls, Crypsys Data Security, importer and distributor of security products and large services providers such as Getronics.

Imports from third countries mostly originate from other European Union (EU) countries (about 25 %), primarily Germany, the United Kingdom and France. Major European suppliers include German software developer Utimaco Safeware AG with a branch office in Arnhem and Sophos Ltd. from the United Kingdom. Some imports of security products from other European countries include products of U.S. origin

that are shipped to the Netherlands from a central distribution point elsewhere in the European Union. Vendors from Israel and the Far East currently have a 10 % share of the Dutch import market. Well-known suppliers with international headquarters in Israel include: Aladdin Software Security Benelux BV and Check Point Software Technologies, both with Dutch branch offices. The main Far East source for security products is Taiwan, particularly for anti-virus software products.

### 17.3.4 Position and Prospects for U.S. Companies

At 65 % of the Dutch $ 160 million import market, U.S. products dominate the market. The U.S. products are seen as representing the latest technology, are of high quality, and are supported by experts in their field. Trade contacts indicated that - as a result of expertise in the security products segment, specifically Internet applications- the U.S. may well increase its current import market share during the next few years at the expense of Far Eastern developers and exporters. Less restrictive export controls and regulations in the U.S. will further stimulate U.S. exports, particularly of encryption products. Best prospects for increased U.S. exports include anti-virus and firewall solutions, encryption and PKI products, managed Internet security services and, in a few years, biometrics solutions.

In addition to U.S. developers that specialize in security solutions such as Computer Associates, Axent Technologies, RSA Security, Inc. Network Associates (McAfee) and Bindview, there are several U.S. companies located in the Netherlands that offer products with embedded security features, e.g. Microsoft, Novell, Netscape, as well as major hardware vendors, e.g. IBM, Sun, HP, SGI, Compaq. These companies are all very well represented in the Netherlands with large offices and extensive distribution networks.

Taking advantage of the Netherlands' favorable location, transportation, communication facilities and skilled workforce, several major U.S. developers of security products have set up their European headquarters and/or distribution centers in the Netherlands. Anti-virus software company Symantec Corp. (Norton products) has its European headquarters in Leiden, near Amsterdam.

## 17.4 Statistical information

Internet use:
1998 - 1.6 million users
2000 - 3 million users
2002 - 7.5 million users

E-commerce (value in U.S. Dollars)
1998 - 310 million
1999 - 1.1 billion
2000 - 2.6 billion
2002 - 10.5 billion

Total E-Commerce market in 2000: $ 2.6 billion

Professional purchases – B2B: 70 %
Consumer purchases – B2C: 30%

At about 60%, the Internet connectivity rate in the Netherlands is among the highest in Europe and growing.
More than 100 Internet Service Providers (ISP's) are active in the Dutch market.
Free Internet Service Providers serve approximately 40% of Dutch Internet users.
Most popular (consumer) products in E-commerce: books, music CD's, software, travel.

Mobile phone use:
1998 - 3.5 million users
1999 - 6.8 million users
2000 - 9 million

## 17.5 Contact information

### 17.5.1 U.S. Embassy Contacts

American Embassy
U.S. Commercial Service
Lange Voorhout 102
1014 EJ Den Haag, the Netherlands
Contact: Mr. Terry J. Sorgi, Commercial Attaché
Phone: +31-70-310 9417, ext. 418
Fax: +31-70-363 2985
E-mail: terry.sorgi@mail.doc.gov
Internet: www.usatrade.gov

American Consulate General
U.S. Commercial Service
Museumplein 19
1071 DJ Amsterdam, the Netherlands
Contact: Ms. Carlanda L. Hassoldt, Commercial Specialist
Phone: +31-20-575 5351, ext. 349
Fax: +31-20-575 5350
E-mail:carlanda.hassoldt@mail.doc.gov
Internet: www.usatrade.gov

### 17.5.2 Internet Security – relevant sites

Dutch Government central Website providing access to all Dutch Government information available on the Internet: www.overheid.nl

Ministry of Economic Affairs: www.info.minez.nl

Ministry of the Interior: www.minbiza.nl

Ministry of Justice: www.minjus.nl

Ministry of Transport, Public Works and Water Management: www.minvenw.nl

FENIT, Federation of Netherlands IT – www.fenit.nl

Vereniging ICT Nederland -Trade Association of manufacturers and distributors of computer and telecommunications equipment: www.v-ict.nl

Association Dutch Information Security Professionals: www.gvib.nl

Association of Netherlands Internet Providers: www.nlip.nl

Netherlands Safe Internet Foundation (established by Netherlands Internet Society): www.sif.nl

Netherlands Internet Society: www.isoc.nl

Internet security: www.veiligophetweb.nl

E-Commerce Platform Netherlands: www.ecp.nl

17.5.3 Tradeshows:

The Internetworking Event 2001
www.tine.nl
RAI Exhibition Center, Amsterdam, The Netherlands
April 18-20, 2001
April 15-18, 2002
Annual professional tradeshow for computer networking.

Business Solutions 2001
www.rai.nl
RAI Exhibition Center, Amsterdam, The Netherlands
September 26-28, 2001
Annual professional tradeshow for ICT solutions, products and services.

Infosecurity 2001
www.jaarbeursutrecht.nl
Jaarbeurs Utrecht, the Netherlands
October 19 and 20, 2001
Annual computer and information security tradeshow.

Internet in Business
www.rai.nl
RAI Exhibition Center, Amsterdam, The Netherlands
November 26-28, 2001
Annual professional tradeshow for Internet and Web development, E-Commerce

Several international trade shows throughout Europe and in the United States are also well attended by Dutch visitors. These include: CeBIT in Hannover, Germany and Systems in Munich, Germany, and Comdex/Fall, in Las Vegas, NV.

Sources used for this survey include information and forecasts from the European Information Technology Observatory 2000 (EITO '00), IDC, Fenit Marktmonitor 2001, Pro Active and various trade contacts, vendors, trade journals and related independent market research studies about the ICT sector.

Exchange Rate: $ 1 = DFL. 2.30

# 18 Norway

## 18.1 Summary

Internet security has not been regarded as a necessity. However, a growing number of viruses and Norway's first cybercrime court cases have made Web surfers as well as corporations realize they must become more security proficient .

The ITC security market was estimated at US$ 110 million in 2000, with significant growth (30-50 percent) expected during the next three years. Most growth is forecast in security authentication, authorization and administration (3A software), while encryption, including virtual private network (VPN), will follow closely, stimulated by expected growth in e-commerce. Sales of anti-virus software (AV) and firewalls will grow 25 percent annually, but Internet service providers (ISPs) and mobile service providers (MSPs) will supply a considerable share of AV and firewall products. There are approximately 15 important IT security vendors in Norway. The U.S. dominates with close to 70 percent of the market.

Heavy use of cellular/mobile phones may boost e-commerce since new communication technology provides consumers with access to Internet. Norway is now actively embracing broadband connections for residential and business usage. The most popular technology as Net users make the transition to broadband is probably cable modems.

## 18.2 Market Overview

Internet has become a very important medium in Norway. In per capita Internet access and utilisation Norway ranks as number 2 out of 55 countries in the world, ahead of the US and behind only Sweden according to the OECD. Norway was the second country to receive the Internet and currently close to 50 percent (2 million) of all Norwegians over the age of 13 have Internet access. There are several reasons for why Norway has been so quick to accept and adopt this medium. As an oil economy, Norway is very wealthy and has the resources to invest in IT. Also, Norway's 4.5 million people have very high telecommunications penetration--57 main lines per 100 inhabitants. All telephone lines in Norway are digital and the country has a very well established ICT infrastructure.

Norwegian companies also have been supplying their employees with PCs to take home, and most of these offers come with Internet access. This is another reason access has continued to increase at such a fast rate during recent years.

The Norwegian ITC market totalled US $ 8 billion in 2000 (trade estimate), and solid growth is predicted through 2001, depending on the world economic situation. The value of IT hardware sales in 2000 was estimated at US$ 2 billion. Sales of PCs are expected to increase after sales fell during 2000 from 630,000 units in 1999 to 550,000.

There are about 15 important suppliers of ITC security products in Norway. U.S. suppliers hold more than 70 percent of the Internet security market. Anti-virus programs are currently regarded as the major ITC security segment, dominated by suppliers such as Symantec and Norman Data Defence, but closely followed by Check Point and Cisco. Encryption software and other security products/concepts are to a great extent supplied by the same companies. Sales of virtual private network (VPNs) for the corporate market tend to be dominated by Cisco, Check Point, Nortel, and Lucent (with its wireless access VPNs).

A recent survey made by the local Computerworld Magazine revealed that even with the widespread use of Internet only 70 percent of Norway's Internet users had AV protection. However, there has been a growing awareness among Web surfers after the "I love you" virus and others were reported in the media, resulting in increased sales of effective AV products.

In order to maintain sales of AV and firewall products, most vendors emphasise VAR arrangements with major ISPs. Most major ISPs now incorporate AV and firewall products as a package to clients, reaching new groups of customers for the vendors. There is a trend towards outsourcing, and vendors also are expanding their business into security management.

### 18.2.1 E-Commerce

As in most countries, electronic commerce is touted as the fastest developing Internet sector. There will be more e-commerce between companies and traditional e-commerce stores. Internet advertising in Norway during 2000 amounted to US$ 120 million, up 80 percent from 1999. As more companies seek to advertise services on the net, e-commerce is predicted to reach US 1.3 billion during 2001, twice the amount recorded for 1999.

However, while dot.com, B2B (e-commerce between companies) and B2C (e-commerce for private consumers) were common IT buzzwords during 2000, there is now talk about m-commerce (mobile e-commerce), which is predicted to reach an amount of just US$ 45,000 during 2001. It is believed that the next generation of security applications will be driven by mobile applications for devices such as cellular phones, WEB phones, wireless handheld computers, and information appliances. Encryption, PKI, authentication, authorisation and administration will become even more critical infrastructure issues as computing goes mobile. New smart card technology is expected to find new end-users in sectors such as cellular telephones, point-of-sales systems, tickets, taxis, etc

A major obstacle to electronic commerce is still a fear about banking and transaction security. Norwegians do not want to give out their bank details over the net. In Norway very few people have credit cards. Banks normally issue debit Visa or MasterCard accounts. As a result, fraudulent use of these cards may directly affect the cash flow of Norwegian consumers. A recent survey among Norwegian Internet users concluded that 71 percent wished to purchase over the network, but only 19 percent had so far done so.

Several new technologies recently have been introduced in Norway to handle security, reliability and speed in electronic commerce operations. Microsoft is very active in marketing and seeking support for its Microsoft Wallet, Site Server, and Commerce Server. Sybase is promoting its iCat system, while Hewlett Packard has recently introduced its Web-Quality-of-Service (WqoS) solution. The Secure Sockets Layer (SSL) standard has been accepted as a safe standard and is currently used in Internet commercial connections, together with credit cards. Electronic coins (i.e. Millicent, Cybercash and Ecash), and Smart Cards, are other money transfer alternatives expected to gain popularity in Norway.

Some Norwegians considered the new Secure Electronic Transaction (SET) standard to be the best operational system in Norway. IBM, Microsoft, VISA and Master Card, among others, recently introduced it to the web browser market. It is a new protocol for Internet transactions incorporating considerable amounts of RSA and Triple DES technology. In Norway, IBM has taken a lead in developing a preliminary SET-based Internet software. They co-operated with Europay (Master Card), VISA, a major Scandinavian centralised bank transaction control agency (Fellesdata), and several local banks, as well as the Internet portal Scandinavian Online, through which most electronic commerce currently is channelled. However, so far only 30 Norwegian Internet shops have adopted the SET system, and the system is said to be too slow, both on the consumer and vendor sides.
However, expected increases in e-commerce will generate a growing need for adequate encryption software in the long term, at least in banking and communications. The U.S. Government recently relaxed greatly export rules for encryption products, but encryption has been, and will likely remain, a tough sell. Corporate firewalls have been the only mainstream commercial products that have thrived in the commercial Internet market. However, Email encryption companies are currently also seeing a change in the wind, at least with some ISPs that might improve slim profit margins by offering an encryption service at a slight premium.

Over 35 percent of the Norwegian public banks through the Internet. This has stimulated more use of encryption technology, including VPNs. Also, several initiatives have recently been taken in the field of personal key infrastructure (PKI) and Smart Card developments:

- **The Norwegian Government** recently passed a law governing electronic (digital) signature, which will be effective on July 1, 2001. This law is based on the EU directive 1999/no.193/EC.

- **Telenor Business Solutions,** a division of Telenor, Norway's major telecom company, specialising in PKI development, has recently bought 500,000 PKI certificates from Entrust (Can). They also hold a reseller agreement with Entrust in

Norway, mainly focused on several **Smart Card** program developments in the mobile phone market.

- Norway's Postal Service has announced intentions to find a PKI platform and the agency is currently communicating with **ID2**, a Swedish company with certificates based on a Swedish PKI standard.

- **Telenor** is curiously awaiting a decision from the Norwegian Banks Payment Services Company (**BBB)**, the market-leading provider of payment services to the Norwegian banks, as to whether they will choose Entrust or other vendors for their PKI program.

- **Proton World** and **BBS,** acting on behalf of the Norwegian banks, recently announced that they had signed an agreement for the pilot implementation of an electronic purse smart card, based the Proton smart card technology in Norway. Under the terms of the agreement, **BBS**, owned by all the Norwegian banks, becomes the Proton licensee for Norway. The agreement marks the first step by the Norwegian banks in their migration to smart cards. The Proton technology platform supports multiple applications (e.g., e-commerce, access control, customer loyalty schemes, telecom calling cards, campus and city cards, health insurance refunds, public transport ticketing, secure Internet payments, etc.). Proton World supports a variety of technologies and specifications to deliver open, interoperable, and global smart card solutions. It is implementing the Common Electronic Purse Specifications (CEPS) along with the issuers of 90 percent of the world's electronic purses, which will ensure worldwide interoperability.

However, awaiting a more secure transaction system demanded by both customers and the growing number of Internet shops, today's form of electronic commerce in Norway is almost entirely based on regular and "risky" credit card payment transactions. According to a recent study, young, highly educated men are most active on the Internet. Three of four people shopping on the Internet are men, although in the last year there has been a 30 percent increase of women shopping on the Internet. Also noteworthy is that a higher proportion of people living in non-urban and remote areas shop via Internet. This is probably because urban dwellers have greater access to specialist shops. Internet usage patterns indicate that Norwegians use the Internet in the morning for information and research purposes, after lunch for communications and e-mail, and in the afternoon for shopping and entertainment.

With these developments in hand, e-commerce is beginning to increase. Some of the most developed concept areas for e-commerce in Norway are still book and CD sales. However, all sorts of purchasing and mail order activities are slowly taking off. One simple way companies are getting around "credit card anxiety" is to send a simple invoice and bank giro to the customer. This concept has advanced into an e-giro in which vendors send invoices directly to the customers through the net.

One of the most promising subsectors in Norway is the development of e-business solutions. However, Norwegian banking practices create some obstacles to full development of e-business in Norway. Other areas showing great promise are Intranet, groupware and workshare programs. Perhaps one of the largest subsectors in

the market is web design for businesses, an area for which PR and advertising companies, ISPs, consultants and graphic designers are all competing.

### 18.2.2 ISP's – MSP's

There is a trend for ISPs to increasingly provide AV protection as a value-added service and thus eliminate the need for corporations and consumers alike to purchase and update these products. Below are names of some of the most important ISPs/MSPs in Norway. Addresses are provided under item 6 – Contact Information.

Internet access primarily is provided through the national telephone carrier, **Telenor.** Telenor recently established two separate divisions (**Telenor Broadband Services** and **Nextra**) to provide net access and broadband services. Telenor has today a significant share of the private and the commercial markets, as well as the mobile market

**Nextra** (Telenor's Internet business subsidiary) is the largest and most dominant Internet service company in Norway with more than 650,000 subscribers.

Swedish **Tele2** is a part of NetCom AB, established in 1993. NetCom is one of the leading telecom companies in Scandinavia. The company operates in mobile GSM service areas, in Sweden for Comviq and Tele2Mobil and in Estonia through the associated company Ritabell. The group operates in public telecommunication and data communication and Internet as Tele2 in Sweden, and subsidiary companies Tele2 A/S in Denmark and Tele2 Norway AS in Norway. Tele 2 is aggressively trying to erode this position by severely undercutting prices and has captured 250,000 customers.

**Online World (Holland)** is another Internet provider with 150,000 subscribers.

**Enitel** was established in 1996 by seven electric power plants to provide Internet services through their fibre optical network built into power lines throughout Norway. The company has 60,000 subscribers in Norway.

**United Pan-European Communications (UPS)** is headquartered in the Netherlands. The company established in Norway in 1997 and has already some 340,000 subscribers to its TV, telephone, and Internet broadband networks

On the commercial side, despite serious market concentration, there is a host of alternative Internet companies. In reaction to high prices for web services to companies by the above mentioned telephone and Internet operating companies, small companies are offering Web Hotel Services. Companies can put clients on the net for a fraction of the price that the telephone operators offer. For just US$13 a month Eye-Publish will provide a company with its own domain name, 10 megabytes of disk space, unlimited transmission and forwarding of e-mail, detailed and graphical web statistics, support for Java and FrontPage etc. In other words, plenty of small mom and pop businesses in Norway will increasingly be serviced by web service companies who do not have the resources to run their own web-server. Firms are increasingly providing solutions to shopping cart systems, product databases, client databases, and simple ordering services, as well as solutions to e-commerce and payment

### 18.2.3 End-User Analysis

Norway's population totals 4.5 million. The corporate market includes some 50 defined major customers, 35,000 large and medium size customers, and 117,000 small companies located throughout the country. The Norwegian corporate market is and will be the most important segment of the ITC security market. The markets break down as follows:

Market Share

| | **2000** | **2001** |
|---|---|---|
| Corporate | 55% | 50% |
| Consumer | 35% | 30% |
| ISP | 10% | 20% |

### 18.2.4 Market Access

The IT security market consisted in 1997 of over 30 suppliers, but strong market consolidation took place in 1998 and several disappeared. The 15 current important suppliers have names that will be recognised as best sellers in the U.S. market. Norwegians are very concerned with having the latest IT technology. Price is not necessarily the most important purchasing factor. Norway does not differ too vastly from other developed countries in its choice of hardware suppliers, and most of the well known software suppliers are here as well, most selling through their own sales subsidiaries. Due to a limited market with strong competition, Norwegian importers, distributors and resellers are very selective in committing themselves to new agent/importer agreements for ITC product vendors. A great number of adequate distributors already hold distributorships and/or reseller arrangements with several large ITC security vendors. Therefore it is often difficult to find a good and hungry distributor or business representative for new-to-market companies, unless they carry proven high tech, state-of-the-art products with good references, and maintain strong back up from the main office. Names and addresses of a few potential importers/distributors are listed at the end of this report**.**

## 18.3 Competitive Analysis

U.S. suppliers dominate the ICT security market with a market share of more than 70 percent. Except for F-Secure (Finland), Trend (Japan), Sophus (UK), and Nortel (Canada) competition from third country suppliers is limited. Most competition is probably felt from a well-established domestic company primarily specializing in AV protection and firewall technology:

- **Norman Data Defence** is by most U.S. Internet security providers regarded as a strong competitor. Norman was established in 1984 and is today an important supplier of data security. With products for risk analysis, virus control, access control, encryption, network security, data recovery and certified data erasure, the company plays an important role as an international player. Norman claims to have 25 percent of the AV protection market in Norway. The company employs about 200, and 2000 sales was reported at US$ 20 million, of which 40 percent was from

overseas markets. Norman maintains sales subsidiaries in many countries around the world. The company also has been awarded several important contracts with the U.S. Government.

### 18.3.1 Regulatory Environment

There are no significant regulatory problems with regard to provision of Internet services. The Government of Norway is doing everything it can to promote the Internet to all groups in society and no official or specific Norwegian law governs imports and sale of encryption software. Import certificates are not required. The Norwegian State controlling agency for encryption software legislation, as well as other EDP related legal matters is **Datatilsynet** (the Data Inspectorate--address below).

Computer software marketed and sold in Norway is free of import duty, but subject to a 24 percent VAT tax. All software products normally are protected under the "Intellectual Property Law's Chapter 11," the Marketing Act, or the Unfair Competition Law. Illegal copying has normally been for internal use and primarily is due to limited information provided by the suppliers. USCS Oslo recommends that American software companies inform and make a very explicit contract with any prospective business partner who would translate, modify, sell, etc., proprietary software in the Norwegian market.

## 18.4 Statistical Information

ITC security software, and anti-virus software in particular, constitutes a considerable part of total software sales in Norway, according to trade sources. Total sale of software in 2000 was estimated at US$ 737 million, of which 15 percent or US$ 110 million was dedicated to ITC security.

The following four major markets with forecasted annual growth from 2000 - 2004:

* Firewalls up 25% annually
* Anti-virus up 22% annually
* Encryption up 40% annually
* 3A software up 58% annually

## 18.5 Contact Information

### 18.5.1 Trade Associations

The Norwegian Computer Society
www.dnd.no
Mølergata 24
P.O. Box 8874 Youngstorget
0028 Oslo

Tel: (47) 22 36 48 80
Fax: (47) 22 36 37 01
Email: dnd@dnd.no

The NCS is the largest special interest society for information technology (IT) in Norway. It is an open, independent forum for Norway's IT professionals and advanced IT users. The society encompasses the IT industry, corporations in general and research and development institutions. The NCS is an independent and wholly self-financed society with more than 15,000 registered members and more than 1,300 company members.

IT Security Forum
Ravnasveien 3
1254 Oslo
Tel: (47) 22 76 38 38
Fax: (47) 22 76 38 48
Email: vivi@pdi.no
Organization established in 1994 to focus on IT security issues. Maintains 150 members interested in IT security from both official sector and private industry.

Secure-IT/IKT-Norge
P.O. Box 546 Skøyen
0214 Oslo
Tel: (47) 22 54 27 40
www.secure-it.org
In 1997 Kontor og Datateknisk Landsforening (KDL), the Norwegian professional and industrial body of the IT industry (see below), created the organization Secure Information Technology (SIT). The board is made up of members from KDL and executives from the IT industry. SIT's mission is to encourage corporations and organisations to focus on computer security by providing information and tools on matters such as computer viruses to inform users of the advantages added security licensed software gives to any organization.

Kontor & Datateknisk Landsforening
(Norwegian Computer and Office Machines Organisation)
Drammensveien 30
P.O. Box 2568 Solli
0203 Oslo
Tel: (47) 22 54 18 02
Fax: (47) 22 44 59 45

### 18.5.2 Trade Journals

IT Bransjen
IDG A/S
www.idg.no
P.O. Box 9090 Gronland
Mr. Paal Leveraas, Editor in Chief
Tel: (47) 22 05 30 00
Fax: (47) 22 05 30 20

Kapital Data
www.hegnar.no
Strandveien 5
P.O. Box 188
1324 Lysaker
Mr. Stein Ove Haugen, Editor in Chief
Tel: (47) 67 58 28 50
Fax: (47) 67 58 28 70

PC World Norge A/S
P.O. Box 90
0567 Oslo
Mr. Bernhard Steen, Editor in Chief
Tel: (47) 22 64 77 25
Fax: (47) 22 68 01 52

PC-Magazine Norge
Fredrik Stangsgate 5
P.O. Box 2795 Solli
0204 Oslo
Tel: (47) 22 12 50 00
Fax: (47) 22 12 50 61

### 18.5.3 Government Agencies

Datatilsynet
(The Data Inspectorate)
Mr. Jorn Arnesen, Manager, Data Security
Tollbugaten 3, Box 8177 Dep
0034 Oslo
Tel: (47) 22 42 19 10
Fax: (47) 22 42 23 50

### 18.5.4 Major ISP/MSP's

**Telenor** is the leading telecom, IT and media company in Norway. From its position as a national telecom operator, Telenor has expanded its area of activities to a broad range of products and services built on and related to electronic communication. The following subsidiaries are important contacts within the fields of Internet security.

**Telenor Broadband Services**
www.telenor.no
Keysersgate 13
P.O. Box 6701 St. Olavs Plass
0130 Oslo
Tel: (47) 22 77 99 00
Fax: (47) 22 77 88 01

**Nextra Norway (Telenor's ISP)**
www.nextra.no

Drammensveien 167
P.O. Box 167 Skøyen
0213 Oslo
Tel: (47) 22 77 19 00
Fax: (47) 22 77 19 10

**Tele2 Norge AS**
www.tele2.no
Ulvenveien 75 A
0581 Oslo, Norway
Tel: (47) 21 31 90 00
Fax: (47) 21 31 91 00

**Enitel ASA**
www.enitel.no
P.O. Box 464
1327 Lysaker
Visiting address: Lysaker Torg 5
Tel: (47) 21 00 00 00
Fax: (47) 21 00 00 01

**UPC Norway A/S**
www.upc.no
Ensjøveien 7
P.O. Box 2842 Tøyen
0608 Oslo
Tel: (47) 21 90 00 00
Fax: (47) 21 90 00 01

**Norman ASA**
www.norman.no
P.O. Box 43
1324 Lysaker
Tel: (47) 67 10 97 00
Fax: (47) 67 58 99 40

18.5.5 Potential Agents/Distributors

Santech Micro Group Norway (SMG) A/S
www.smg.no
Mr. Axel Jensen, Managing Director
Lysaker Torg 25
1366 Lysaker
Tel: (47) 67 11 40 00
Santech Micro Group AS is a major ITC distributor connected with more than 3,500 retailers in Norway. The company has 150 employees and annual sales of US$ 22 million.

Eterra A/S
www.eterra.no
Mr. Per Morten Sandstad, Product Manager

Brynsalleen 2-4
0667 Oslo
Tel: (47) 22 09 50 00
Fax: (47) 22 09 50 01
Eterra is a Nordic internetworking company within the Merkantildata group of companies comprising 3,200 employees specialized in designing, building, implementing and operating innovative communications, infrastructure and network solutions

SC Norge
www.mamut.com
P.O. Box 66
1404 Siggerud
Tel: (47) 98 86 25 10
Small company established 1997 specializing in IT security products. Employs 4.
Represents Mamut.

Sospita AS
www.sospita.com
Gjerdrumsvei 10c
0484 Oslo
Tel: (47) 815 49 090
Fax: (47) 815 49 091
Founded in Norway in 1995 under the name Protective Technology, Sospita provides the software industry and its users with software license protection based on a tamper-proof device (e.g. smart card or token). The company goal is to protect intellectual property owners from losses associated with software piracy, by offering cost-effective and flexible licensing solutions with an unparalleled level of security. Represents Gemplus (Luxemburg).

FOR ADDITIONAL INFORMATION CONTACT:
Commercial Service
US Embassy
Drammensveien 18
0244 Oslo
Tel: (47) 21 30 88 34
Fax: (47) 22 55 88 03
Attn: Sebastian Remoy, Senior Commercial Specialist
Sebastian.Remoy@mail.doc.gov

# 19 Poland

# 20 Portugal

## 20.1 Summary

Internet security has not yet registered severe problems in Portugal because until recently it had not been really necessary. The large majority of internet traffic does

not need security measures, and the minimal part that needs it, such as credit card number transfers, was easily solved with SSL (Secure Sockets Layer protocol). The SSL protocol was used successfully by major websites doing credit card transactions.

If Internet is supposed to be used as the basis for electronic commerce between companies, the question of safety has to be approached from a different direction due to the potential danger it may bring.

In the future digital signatures will be the safety basis of Internet. As in the other EU countries, Portugal adopted the legislation that equals/compares both digital and manual signatures and establishes the way on how digital signatures will be implemented inside the European Union.

During the course of 2001 it is expected that digital signatures acquire a legal statute not only in Portugal but also throughout Europe. This process will allow the possibility to negotiate and sign contracts in the Internet, as well as change electronic documents of any kind fully secured.

In terms of data privacy the United States recently initiated high level negotiations the EU with the goal of ensuring the free market flow of data and effective protection of personal data.

These discussions led to the development of the Safe Harbor framework based on principles that closely reflect the US approach to privacy, and at the same time meet the EU directives adequate requirements. The European Commission agreed that these principles were adequate in July 2000 the Safe Harbor became effective on November 1, 2000.

The Safe Harbor applies to all personal information transferred from the European Union whether collected on or off line and within the scope of the directive. Decisions by US organizations to enter the Safe Harbor are entirely voluntary.

The EU has agreed to allow US organizations time to consider whether or not to participate in the Safe Harbor and, if so, to implement privacy policies to put the principles into effect. As such, EU member states have also agreed to avoid interruptions in data flows, so as not to call into question the good faith efforts being made to secure adequate protection for data transferred from EU.

The Safe Harbor either eliminates the need for prior approval to begin data transfers or provides for automatic approvals. These principles offer a simple and more efficient means of complying with the adequate requirements of the Directive, which should specially benefit small and medium enterprises.

# 21 Romania

## 21.1 Summary

Internet penetration in Romania is currently quite low by European standards, but the market has a dynamic development. The support of the Romanian Government, which has just launched a strategy aiming at the rapid growth of the IT segment of the economy and envisages a series of major programs directed mainly at education and public administration (e-government), will contribute importantly to increasing imports of Internet-related products and services. Best Internet Security market opportunities for U.S. companies include knowledge management, public key infrastructure, and smart cards.

## 21.2 Market Overview

### 21.2.1 Introduction

Internet penetration in Romania is currently small (1.5% of population, i.e. about 350,000 users), but the growth rate of the sector is significant (5-6% per month). There are over 150 ISPs. Computer literacy and good English language skills of the population, the existence of a widespread cable TV network (about 3 million subscribers) and the very good penetration (about 9%) of mobile telephony (as a basis for mobile Internet) are factors which will support increased Internet access. Factors negatively impacting Internet and e-commerce development include the insufficient number of PCs (only about 750,000 for a population of 22 million, but growing at an annual rate of 30%), limited use of credit cards, and high fees charged by the national wired telephony operator, Romtelecom, for the use of its lines. Since Romtelecom's monopoly will end on December 31, 2002, it is expected that rates will decrease substantially once the market is fully liberalized. The substitute for Romtelecom's phone lines is coax cable. Cable TV companies have networks in all cities and in many rural areas. Large cable TV operators already offer Internet over their networks. Internet users are concentrated in the larger cities (Bucharest, Cluj, Timisoara, Iasi). Home users rely mostly on modems; institutions (schools, universities, foundations, etc.) are generally connected via dedicated lines; and business companies use both cable and dial-up connections.

As regards e-commerce, currently there is only “e-ordering” in Romania. Due to the incomplete legal framework, the Internet link between the supplier’s server and the server of the supplier’s bank (that would enable an e-transaction to take place with financial risk covered by the bank and traceable responsibility on the customer) does not exist. Currently, the workaround involves either a POS and some additional operations or physical invoicing/payment. There are at least five portals in Romanian providing listings of links by categories and search engines. Some of them provide news content as well as e-commerce B2C offers. In most cases, the contents and the search engines are of poor quality. The use of credit cards in Romania is in its initial stages. While the number of stores that accept payment by credit card increases, the customers are not yet well educated regarding their use. Most banks lack the infrastructure necessary for clearing payments by Internet. However, major banks already average about 250,000 credit card users per bank.

### 21.2.2 Internet Security Market

#### *21.2.2.1 Authentication*

User name and password represent the most widely used procedure. Lately, the use of files on diskettes as an additional "key" has been catching. For the dial-up connections, the "call back" authentication system is becoming increasingly popular. Password and SSL seem to represent the current trend. These solutions are implemented by several companies, which consider them to be reliable. The military segment of the market, which is more advanced, uses smart cards.

#### *21.2.2.2 Authorization*

This activity is closely related to the functions of the System Administrator. See below.

#### *21.2.2.3 Administration*

A rather high number of skilled, well trained, experienced, and certified (MS CSE, Novell CNE and CNA) personnel are available. They have very good technical skills, but lack discipline and good management/procedures. The software solutions used include the administration component of the operating systems for servers (MS and Novell are the most used), as well as other additional dedicated solutions (MS SMS -- by far the most popular, with about 20 implementations -- HP Open View, Tivoli). About six local companies, led by GeCAD and Prosoft, act on the market for consulting and services related to administration. Currently there is no such position as a "Security Manager" with local companies. Security functions are the responsibility of the System Administrator.

#### *21.2.2.4 Secure transactions*

The use of SSL and VPNs is relatively new, but has been constantly growing over the past two years.

#### *21.2.2.5 Firewalls*

All the ISPs are promoting firewall-type solutions (Cisco and MS/Proxy Sv.). Linux solutions are also widely spread. On the hardware side, Cisco is the leader, although their solutions are regarded as rather expensive. Approximately 12 companies are active in sales, consulting, and services related to firewalls.

#### *21.2.2.6 Virtual private networks*

Such networks are used by many companies, but with little efficiency due to bad management (i.e. the technology is in place, but it is used unwisely). The local leaders on this segment are Logic Telecom, Global One (Cisco), Online Services (MS), and a Swiss company that is very active with military-type clients.

*21.2.2.7 Intrusion, detection, and monitoring*

All ISPs are highly interested in these issues. One of the major local ISPs has even hired a team of "crackers" whose job is to attempt to crack its nets to identify vulnerable points. Professional intrusion monitoring and information backup are common practices for foreign companies operating in Romania.

*21.2.2.8 Knowledge management*

Some document management and workflow management solutions are the only components currently in place. There are less than 20 implementations from Siveco (France), Ultimus (USA), Documentum (USA). Knowledge management is considered to be an important export opportunity for U.S. companies, as banks and large government-owned operations are starting to express a need for it. Local companies have expressed interest in commercially representing American suppliers of such solutions.

*21.2.2.9 PKI*

Public key infrastructure is also considered as a hot business opportunity in Romania. Banks are quite interested in getting affiliated with Verisign and the like, as they are ready to start e-transactions. A relatively high number of local companies have proven technically capable to implement respective MS solutions, while a few solutions from Baltimore Co (USA) and Entrust (Canada) have also been used.

*21.2.2.10 Encryption*

Because of the lack of any legislation/regulations addressing the issue of encryption, currently there is a significant vacuum on this market segment in Romania. Until regulations are enforced, there is a good likelihood for honest business to circulate their sensitive data with no encryption and, on the other hand, for companies practicing bad business to encrypt their data and skip control. Import and export of encryption algorithms is not regulated either, with all the respective implications. For data transfer, PGP from McAffee is quite popular, but it is used with no proper coordination, the same being true for SSL of FSecure. Encrypting stored data is not a common practice.

*21.2.2.11 Smart cards*

This segment will probably provide best export opportunities over the next two years as it is expected to show significant rates of growth in the Romanian market. The Government and its various structures, the large and expanding network of gas stations, as well as social security bodies issuing the so-called "social cards" are some of the most important and immediate prospect customers of the respective products and related services. Imports of smart cards from SCI (USA) have started, and development of locally designed software solutions for smart cards is already considered good business. As Windows 2000 (designed to recognize smart cards) is a highly popular operating system, MS is strongly promoting the concept and its rapid implementation.

#### *21.2.2.12 Content screening, anti-virus and mobile code*

As anti-virus software products have already gone beyond the anti-malware stage and are well into real “security suites”, all top five anti-virus products in use in Romania (RAV AntiVirus, Norton AV, McAffee AV, KAV, and Fsecure) have highly effective built-in features for both anti-virus search and content screening. The market demands such solutions and the topic is very seriously regarded, especially in organizations sensitive to mission critical situations. An average of 2.2 different AV solutions per computer are implemented in the information systems in the corporate sector in Romania. With the continuous growth of the PDA segment (approximately 400 PDAs in use in Romania), suitable security suites (mostly AV solutions) have triggered more and more significant demand. All international market leaders (FSecure, TrendMicro, McAffee, GeCAD) are important players on the Romanian market. GeCAD, a Romanian-American AV developer, has developed a solution for Psion’s "Epoc" operating system.

#### *21.2.2.13 Data warehousing and information*

Compaq is the market leader in Romania in such services. The market develops along with the strengthening of the enterprise segment.

#### *21.2.2.14 Enterprise security*

Enterprise solutions are in great demand, and at least 6 local companies are active in providing them. Solutions from MS are the most popular. Foreign companies operating in Romania are the most advanced in this regard, while large Romanian companies are just starting to acknowledge the need and act accordingly, but in a disorganized manner, their first concerns being anti-virus solutions and firewalls.

### 21.2.3 Legal Framework

The policy of the Romanian Government is to encourage access to Internet. The Ministry of Communications and IT has recently drafted laws on e-commerce, e-signature, anti-fraud, and personal data protection. These laws are expected to be passed by Parliament by mid-2001. The proposed legal framework also includes laws on electronic documents and archives, electronic notary, and electronic public administration, as well as regulations applied to banks, insurance, and capital markets. The Romanian Government has not yet developed a policy, and pertinent legislation, on the use of encryption products.

# 22 Russia

# 23 Slovak republic

# 24 Slovenia

## 24.1 Summary

Rapid Internet growth in the late nineties slowed down in 1999 and 2000 in Slovenia. A relatively high penetration of 300,000 users or 15% reached in 1998 decreased in 1999 and peaked up again in fall 2000. On the other hand, companies are expanding their use of Internet. A vast majority of companies have an access to the Internet, and most of large and medium companies have created their own web page. The market leader is the service industry, which started with Enterprise Resource Planning (ERP) and Customer Relationship Management (CRM) systems. Banking and insurance sector, state administration and telecommunications were the fastest developing IT sectors in the last two years. Investment in IT technologies reached USD 350 million. The number of home users dropped in 1999 and started peaking up again in the fall of 2000.Internet sales grew year-on-year by 450% in 2000, amounting to still very moderate USD 1.2 million.

The Internet has started to become the most important business platform, enabling connectivity to all e-business players: customers, partners, suppliers and employees. The first generation of e-business applications focused on navigation and speed, while the new generation demands security, reliability, availability, and performance. This brings enormous opportunities to companies delivering innovative solutions. Security solution could be handled as standalone product, as a security site, or fully integrated with e-business infrastructure management solution. The up-to-date solutions must include risk assessment, attack detection, loss prevention, and support key industry standards. Security solutions, that are part of the larger task of enterprise management are protecting infrastructure and power the e-business. The solutions securing the e-business include intrusion detection, administration, authentication and authorization, and VPN (virtual private networks). With seamless platform coverage, the solutions provide comprehensive, end-to-end security.

Companies, delivering security solutions, are holding considerable share of the IT market. Innovative solutions are built on up-to-date HW and SW platforms, and integrated with solutions available on market. Market for security solutions is very competitive and open also to small and mid-sized companies. Its international character forces companies to follow new trends and meet high standards. Local Slovenian companies are holding very strong position in delivering complete solutions that meet needs of individual clients. There is a great opportunity for the U.S. firms to distribute their security solutions via local value added distributors or select local software developers to deliver solutions based on U.S. companies' security products.

The Republic of Slovenia closely follows all international trends in data protection legislation. All EU directives are followed. Slovenia was among the first countries adopting a bill on electronic signatures in September 2000. The certification practice is still sporadic, but the government solution is expected in the next twelve months. Several commercial issuers of certificate – certification authorities (CA) exist following the EU framework for development of Public Key Infrastructure (PKI) certification practices.

## 24.2 Market Overview

The market for security solutions and services has been growing rapidly in the past year, following the fast development of IT and telecommunications, especially 100% digitalization. Leading sectors are banking, insurance, telecommunications, state organizations and retail business. A few dominant Slovenian banks are constantly among early adopters, including SKB with first e-banking solutions back in 1997. All state organizations are now fully Internet equipped.

The growth of needs has brought opportunities for companies active in delivering security solutions and related services, such as system integrators, software developers, value-added distributors and application service providers. In the security sector, up-to-date information on methods, legislation and solutions is on a very high level. The sources of information are trade fairs, conference, specialized events such as company presentations, and Internet. Majority of companies are aware of the fact that the security solutions are on-going process that has to be continually developed. Complete firm's security solution could be built in steps, from installation of firewall, VPN, anti-virus protection, further to include encryption, two-phase authentication, digital certification and PKI, and should be completed by intrusion detection, network monitoring and performance measurement.

### 24.2.1 Market Segments

The following products are currently available on the market, as components of innovative security solutions:

- Firewall: firewall is the basic component for network protection from non-authorized user. There are two types of firewalls: packet filters and application gateways. Most of solutions are built for UNIX system. The most comprehensive solutions include the best world SW like CheckPoint and similar.
- Virtual Private Network (VPN): VPN provides safe communication with open networks, such as Internet. It enables safe communication with company branches, managers on business trip, company suppliers and clients. VPN solution provides encryption of communication channel and user authentication.
- Anti-virus protection: a wide portfolio of anti-virus programs is being offered.
- Intrusion detection: the method of intrusion detection is based on server that controls and analyses network performance.
- Authentication: authentication method implements mechanism of user identification. Strong authentication, used in banking and payment systems, requires two items to be identified independently.
- Encryption: encryption method is used for defining user rights. Encryption system protects network from outside and inside intruders, and enables to create private environment for individual user. Encryption systems range from off-line encryption (files encryption), disks encryption, to encryption keys of different lengths. A 128kb encryption is a standard, based on VeriSign or Microsoft solution.
- PKI (Public Key Infrastructure): PKI is a method of identification and certification of individual user from large group of users. The PKI infrastructure is

a complex solution that enables user identification and certification of his electronic signature.
- Data warehousing: data warehousing has been recognized as good technology and great business opportunity by the first two companies which have already started offering the service.

There are many local firms that implement security solutions. They mainly provide solutions in order to fulfill all customers' needs. On the other hand, there are only a few IT companies with strong security departments. They target to a certain group of clients. The implemented solutions combine several security methods. Most of solutions are based on Microsoft NT technology or LINUX. PKI based solutions are usually targeted at large and medium-sized companies that require implementation of VPN. Certificate Authority is mainly based on the Entrust PKI technology.

A few large accounts (banks, Telekom Slovenija) have strong IT departments and often develop their own security solutions with latest versions of best available HW and SW.

There are six certificate agencies in Slovenia. Four are using American products for implementation, while two are developing their own product. A national agency establishment is expected soon, because a very small market can not justify financial inputs in so many separate developments.

### 24.2.2 Major trends, drivers and obstacles

The market growth for security solutions has been following the very fast development of IT sector. It seems that the security sub sector will be among top growth drivers for the industry in the near future. Local firms have proved a very high qualification for development of application software, build on standard products, available on the market. U.S. products hold the leading position in all IT market segments. In the application software development, close partnership with manufacturers and software developers is essential. U.S. security systems often set up an international standard that has to be met in individual solutions.

Market is driven by rapidly growing needs. The leading IT spenders are looking for solutions that bring system efficiency and/or enable them to go to e-business. Especially fast growing sector is banking. Among others there are some good examples in retail business, telephony, electronic distribution of legal and business data, etc.

The IT market is supported with relatively good telecommunications infrastructure with 100% digitalization in 2000. Slovenia lacks better international links. Access to Internet is available via dial-up, leased line, wireless connection and cable TV. There are 6 large ISPs with international connectivity covering the majority of the market. A number of ISPs that expand their services to become Application Service Providers – ASPs is growing. Their services include a high level security solution when communicating with clients.

There are no import obstacles hindering the security market development. Imported HW and SW products, including encryption software are not subject of duty rates or any import limitations on the Slovenian side.

High telephone tariffs and high costs of leased lines have caused some obstacles, especially for small companies and home Internet users. The forthcoming demonopolization of fixed telephony and increasing competition in mobile telephony will hopefully remove those obstacles.

Low trust or even customers xenophobia is a serious obstacle that has to be overcome by increasing level of information and by adoption of adequate legislation.

## 24.3 Competitive Analysis

The market for Internet security products is very competitive. The key factor is up-to-date design, that supports frequently used HW and SW platforms and integrates with solutions of wide range of technology partners, providing flexible solution for reasonable price.

Security solutions are distributed and/or implemented by local companies with very professional personnel. Value added resellers and system integrators usually build in a piece of their own knowledge into final solution.

U.S. companies dominate the Internet security market. Local companies work closely with world top producers from the United States and a few others like French ActivCard and some Israeli companies.

## 24.4 Contact Information

### 24.4.1 Legislation

Ministry of Information Society
Langusova 4
1000 Ljubljana
Slovenia
Tel + 386 1 478 8223; fax + 386 1 478 8142
Dr. Pavel Gantar, Minister
mid@gov.si

### 24.4.2 Security Solutions Key-players

HERMES PLUS Group – ICOS
Slandrova 2,
1000 Ljubljana
Slovenia
Tel + 386 1 5895 256, fax + 386 1 5895 259
www.hermes-plus.si

HERMES PLUS Group – Macek Communications
Kersnikova 19
3000 Celje
Slovenija
Tel + 386 3 428 4000, fax + 386 3 428 4010
www.hermes-plus.si

Hermes SoftLab
Litijska 51
1000 Ljubljana
Slovenia
Tel. + 386 1 586 5200
www.hsl-ic.si

MIBO
Zelezna 14
1000 Ljubljana
Slovenija
Tel + 386 1 473 5310
www.mibo.si

NIL
Einspielerjeva 6
1000 Ljubljana
Slovenia
Tel + 386 1 474 6500
www.nil.si

SRC.SI
Trzaska 116
1000 Ljubljana
Slovenija
Tel + 386 1 242 8000
www.src.si

# 25 Spain

# 26 Sweden

# 27 Switzerland

**1. Summary**

Switzerland is one of the most computerized countries in the world. It spent $17 billion on information and communication technology in 2000 and a 7 percent growth is anticipated for this year. This ranks Switzerland as number 1 in the world, followed by the United States and Scandinavia. Despite its relatively small size, it is seen as an attractive, highly developed and competitive market in Europe. This level of computerization is in part due to the presence of sophisticated industries and an active business and service sector. These groups rely heavily on computers to reduce labor costs and to compete effectively in the international market. Switzerland is also a host to a number of international organizations such as the United, and regional or world headquarters of multinational corporations. These in turn create a demand for the latest in computer and communications technology.

## 2. Market Overview

Increased Demand for Internet Security Solutions

About 2.5 million Swiss households are equipped with computers, and experts estimate that in the year 2000, about 40 percent (3 million) of all households will have internet access. Switzerland boasts about 150 providers of direct Internet connections. Growing acceptance of this medium can also be evidenced by an increasing market volume of services for interactive computing, TV sets and internet access, which is projected to rise to $ 0,5 billion in the year 2000, up from $ 0,3 billion in 1998.

Swiss businesses had invested approx. $ 0.25 billion in net access by mid-1999 and at the current pace over 60 % of all Swiss companies will soon have Internet sites.

Market insiders expect a considerable growth in software and services for Internet security. Internet security software sales amounted to around $ 140 million in 2000. This volume is expected to reach $ 650 million in 2003. The worldwide market for security software and services reached $ 5,2 billion in 2000 and is expected to reach $ 9 billion by 2003.

Anti-virus programs, firewalls and encryption-software account for the largest part of this segment. However, many decision-makers and IT administrators are still not prepared to invest large amounts of money into net security, which is partly based on a lack of information about available tools and how to use them.

Online-Shops: 90 percent are on the edge of the law

**Developments in E-Commerce are not as positive as overly optimistic experts predicted earlier. Reasons are, among others, the lack of customer satisfaction with web sites and potential security risks in data transfer.**

A recent study researching over 100 online-shops showed that nearly all of these shops had security problems. A scan of net security revealed poor results: Only 5 percent of the researched networks were without faults, which means that hackers and

have virtually free access to a multitude of domains and shops. Potential attackers do not even have to be very skilful.

Data protection, which has always been a big issue in Europe as a whole has also been neglected by the majority of the surveyed internet-businesses:

- 97% of online shops do not inform customers about data protection
- 86% do not ask customers for their consent when using their personal data
- 43% do not name the purpose for the data inquiry
- 93% do not guarantee that data will be deleted once the transaction is completed
- 63% do not inform customers about contract rights
- In 82% of the shops the General Terms of Business are not effective (because there is no consent from the customer to the General Terms of Business)
- 68% do not cover the costs for return delivery (and in doing so the Remote Sales law is ignored)
- 48% do not give a final price for the content of the shopping trolley
- 70% only offer one method of payment
- 44% do not name any personal contact on their website

**3. Competitive analysis**

Swiss customers tend to be more cautious in embracingE-commerce solutions than their counterparts in the United States. Research conducted last year by BCG shows that most online shoppers pay by credit cards (45 %) or by invoice (40 %). Only 2 % of all payments were done by e-cash. The 55 out of 100 customers who refuse to use their credit card still shows the immediate need to make financial transactions “feel” safer for the consumers.

The Swiss software encryption industry has a relatively large world market share and competition in the Swiss market is increasing. The firewall software segment is highly competitive and may have reached saturation. Intrusion detection tools (stealth system software) are in their early stages of development and offer good potential. (These tools raise an alarm as soon as there is an attempt to bypass security installations.)

**Export Control of IT-Security products**

Import and use of encryption products is not limited. Exports, however, are regulated by the Wassenaar-Agreement, in which more than 30 States agreed not to supply technology for the production of weapons to certain countries. Encryption products fall under the category of Dual Use Products. The Wassenaar Agreement has to be implemented via national legislation. Within the EU, this is based on the EG-Dual-Use Ruling NR. 1334, of September 2000.

**4. Statistical information**

Switzerland has the highest per capita spending on ICT in the world. 3,5 million Swiss are using the Internet today and they projected growth for 2001 is another 8 %. The ration between female and male Internet surfers is 63 vs. 37 %. Most users are still in the age bracket of 14 – 29. While virtually all large Swiss companies use the Internet, only 30 % of the small and medium enterprises (SMEs) are online (year 2000 status). 14 % of the Swiss SMEs are planning to implement Internet access in the short, but a staggering 56 % of all SMEs don't use the Internet at all.

About 10 % of the Swiss population use Internet banking – this is approx. twice the rate of the European Union. However, yearly spending on the Internet is still at only $ 80 compared to $ 400 in the United States (based on 1999 figures).

In the euphoria about B2B, B2C has been neglected. While there is growth potential in both sectors, B2B generates 80-90 percent of e-commerce revenues, and especially virtual marketplaces are becoming increasingly important. Worldwide B2B volume is predicted to reach $ 109 billion in 2004, compared with $ 2.1 billion in 2000.

## 5. Contact information

1. Federal Department of Transportation, Communications & Energy
   Dr. Hans Werder, Secretary General
   Kochergasse 10
   CH-3003 Bern
   Tel: (41-31) 322 5506
   Fax: (41-31) 324 9622
   URL: www.admin.ch

2. Swiss Communications Commission
   Dr. Fulvio Caccia, President
   Marktgasse 9
   CH-3003 Bern, Switzerland
   Tel: (41-31) 323 5290
   Fax: (41-31) 323 5291
   www.fedcomcom.ch

3. Swiss Federal Office for Communications
   Mr. Marc Furrer, Director
   Zukunftsstrasse 44
   CH-2501 Biel, Switzerland
   Tel: (41-32) 328 5511
   Fax: (41-32) 328 5555
   www.bakom.ch

**Associations**

SWICO (Swiss Information and Communications Association)
Technoparkstrasse 1
8005 Zurich, Switzerland
Tel: (41-1) 445 3800
Fax: (41-1) 445 3801
E-mail: swicomail@swico.ch
URL: www.swico.ch

SIMA (Swiss Interactive Media Association)
PO Box 1211
8032 Zurich, Switzerland
Tel: (41-0878) 800 124
Fax: (41-0878) 800 125
E-mail: admin@sima.ch
URL: www.sima.ch

**Trade Shows**

The most important means of trade promotion in Switzerland are trade fairs, conferences and seminars. Swiss executives in this industry sector attend the annual communications and computer show CEBIT in Hannover, Germany, held in March each year.

The most important Swiss trade events for displays and promotions are listed below:

1. Orbit/COMDEX Europe – major autumn conference and exhibition for the European IT industry (the next event is held in Basel from September 25 to 28, 2001).

Contact:

Orbit Industries Fair

Mr. Walter Gammeter

P.O. Box

CH-4021 Basel

Tel: (41-61) 686 2250

Fax: (41-61) 686 2189

E-mail: wgammeter@messebasel.ch

URL: www.orbit.ch

2.INTERNET EXPO (iEX) -- annual trade show, usually held in February (next event is held in Zurich from February 6 to February 8, 2002)

Contact:

Compress Information Group

IEX 02

Seestrasse 99

8800 Thalwil, Switzerland

Tel: (41-1) 722 7700

Fax: (41-1) 722 7701

E-mail: info@iex.ch

URL: www.iex.ch

**Commercial Service Contact:**

Ernst (Aschi) Hegg
Information & Communication Technology Specialist
U.S. Commercial Service (U.S. Department of Commerce)
American Embassy
P.O. Box
Jubilaeumsstrasse 93/95
3001 Bern
Switzerland
Tel: (41-31) 357 7343
Fax: (41-31) 357 7336
E-mail: aschi.hegg@mail.doc.gov
URL: www.buyusa.com
URL: www.uscom.ch

# 28 Turkey

## 28.1 Summary

With over 1.7 million internet users in 2000, and expected exponential growth reaching 6 million users in 2002, internet security in Turkey is in its infancy stage. At the moment, two major banks (i.e. Garanti Bank and IsBank) are the only banks setting up credit card encryption programs for e-commerce sites. With start-up costs ranging between USD 2,000-3,000 just to set up the credit card verification system with the bank, it is no easy task for e-commerce entrepreneurs.

Although start-up costs for e-commerce sites in Turkey are high, nearly every bank markets “internet banking” to their customers. This multi million dollar investment in the IT sector has not only enabled customers to enjoy banking from home, it has significantly furthered a trust in e-commerce transactions.

Although banks have been the leaders in pushing the envelope for internet security in Turkey, other financial institutions, such as www.ataonline.com.tr, a brokerage house, have adopted and successfully deployed systems to monitor and execute buy/sell transactions on the Istanbul Stock Exchange.

Monitoring and protecting networks and internet sites looks to be a significant market trend that will parallel the development of e-commerce in Turkey. Increased threats by hackers along with the proliferation of destructive virus related programs have increased the demand for firewalls and other safeguarding applications.

### 28.1.1 B2B

"Business To Business" (B2B) applications in Turkey are very limited. Presently, only a few companies provide entrepreneurs the opportunity to have their own e-commerce websites on a turnkey basis. Ticaretnet, a web services firm, (www.ticaretnet.com) assists companies to start their own Website within Ticaretnet's servers. Ticaretnet provides subscribing firms a shopping basket and credit card authentication. However, this venture is not suitable for small or medium sized companies wishing to be on the net. Ticaretnet's solutions target larger companies thus leaving a gap in the B2B market.

Other e-commerce success stories, such as buying a car, conveniently obtaining consumer products/service - including purchasing airline tickets via the net, are simply not yet occurring in Turkey. However, banks and stockbrokerage companies such as Pamukbank (www.pamukbank.com.tr) and Ata (www.ataonline.com.tr) have recently started online brokerage services for stocks traded on the Istanbul Stock Exchange.

Another important B2B application that is generating more revenues each day is advertising on the internet. Although the exact breakdown and characteristics of what is being advertised on the net are unknown, a recent study characterizes the sectors / products immediately conducive to net advertising as follows: computer products 38%, durable goods 20%, media 17%, telecommunication 9%, finance and banking 6%, and miscellaneous others 10%. Banner exchanges between companies and popular websites are becoming a popular new trend in net advertising.

The advertising trends indicate that technology oriented industries, such as computer companies, banks, and electronic consumer goods manufacturers understand the importance of the internet and are committing advertising dollars to the net.

### 28.1.2 B2C

"Business to Consumer" (B2C) sites are rare, but the investments are considerable. Small and medium sized enterprises (SME's) are sparsely represented on the Internet in Turkey. Instead, large companies have realized the importance of e-commerce and offer their goods on the internet. Examples of B2C sites include Internet Bazaar (www.internetbazaar.com), which imports U.S. products from catalog companies such as JC Penny, Sears, LL Bean etc.; Kangurum (www.kangurum.com.tr), a virtual mall owned by Koc Holding; Migros (www.migros.com.tr), a Koc Holding owned

leading supermarket chain that offers groceries delivered to the consumer's door; Remzi (www.remzi.com.tr), a bookseller; Photo-Market (www.foto-market.com), providing photography products on-line, and Sanal Carsi (www.sanal.carsi.com), a department store selling its wares in cyberspace.

### 28.1.3 E-Government

"E-government" is desperately trying to keep pace with the private sector. Many government websites such as the Foreign Trade Undersecretariat (www.foreigntrade.gov.tr) Ministry of Foreign Affairs (www.mfa.gov.tr), and the State Planning Organization (www.dpt.gov.tr) offer precise information regarding statistics and practices on their site. E-government is breaking new ground in other areas as well, such as posting the results of state organized university exams on the internet. While sophisticated informational websites can be found at various Turkish Government agencies, practices such as e-procurement are not yet available. However, efforts continue to resolve the issue of electronic signature, which will enable citizens to process taxes and other official transactions.

#### *28.1.3.1 Virtual Communities*

Virtual communities are gathering under major Internet Service Provider (ISP) sites such as Superonline (www.superonline.com), Ixir (www.ixir.com), and Garanti Bank (www.garanti.net). Ticaretnet, the B2B service provider, is trying to gather companies under one business-oriented roof. These sites have all the common virtual community attributes including chat rooms, yellow pages, e-mail accounts, news, and sports.

Commercial banks in Turkey are at the vanguard of another trend. Banks offer services through the internet allowing customers to pay bills, buy and sell stocks, exchange currency, as well as transfer money and use other bank products. Some banks have successfully increased their customer portfolios through internet banking. Garanti Bank (www.garanti.com.tr), Osmanli Bankasi (www.osmanli.com.tr), Pamukbank (www.pamukbank.com.tr), Yapi ve Kredi Bankasi (www.yapikredibank.com.tr) and IsBankasi (www.isbank.com.tr) are the more successful practitioners of this new internet banking trend. These banks have invested large sums in internet resources allowing the firms to act as ISPs for their customers.

## 28.2 Market Overview

The security market is just beginning to grow in Turkey. Products such as Norton Antivirus and McAffee are the only common programs that are used by PC owners as well as small to medium sized businesses. Larger companies usually seek the help of software houses such as Likom Software or Koc Systems for more customized solutions.

### 28.2.1 Intrusion, detection and monitoring

The banks and financial institutions at the leading edge of e-commerce in Turkey have not implemented Internet monitoring. After the initial setup of a firewall, most organizations are not sure as to what happens when thousands of users try to log on at the same time, or how they could optimize download times given the vast variables within their systems. One US based company, Mercury Interactive, has seen the opportunity in the market and has acted quickly to set up an office in Istanbul. The firm reported that it is surprised by the amount of interest its products have received by the Turkish IT market.

The Government of Turkey does not regulate issues such as authentication, authorization and administration between parties. Although plans are underway to establish a regulatory body regarding e-signature, e-certificates and monitoring, no such regulations exist today.

### 28.2.2 Secure transactions

The most common method employed by banks to secure internet banking transactions with their clients is based upon an e-certificate that is downloaded by the customer. Once this download is completed, only computers that have the e-certificate permit the customer to complete transactions via the internet. The e-certificate process involves frequent prompts for a password and username before and after each transaction. Securities brokerage houses do not use the e-certificate system that enables customers to complete transactions via a password and username only. Universally, the brokerage firms describe their customers as “on the move” and dismiss the concept of tying the client to using only one computer as required with the a e-certificate system.

In addition, nearly all the sites offering banking and brokerage services via the internet employ voice authorization systems requiring users to punch in their password over the phone in order to have the transaction processed.

### 28.2.3 Enterprise security, Firewalls & Private networks

Private networks remain the favorite protection method for companies to assure security between their in-house network system and the internet. Intranets are increasingly popular among large companies as they allow employees fast access to the companies’ own websites as well as emails etc. Some companies choose to totally separate their networks from the internet by issuing one computer per person for the company intranet and one computer per several persons for utilizing the internet. This approach saves time and money otherwise invested in firewalls and support personnel. Knowledge management is usually performed by the IT department in the larger firms and often outsourced by medium size companies.

### 28.2.4 Encrypton

Encryption remains the number one mystery of the Turkish IT market. No regulation has yet been established concerning importing, exporting or the implementation of encrypted software. The general notion is that products with encryption embedded in

the application are regulatory-trouble free. However, pure encryption products are less likely to be permitted into the country.

### 28.2.5 Smart Cards

A multi-million dollar project is on the drawing board to be implemented by the Ministry of Health regarding smart cards. The project goal is to provide every Turkish citizen subscribing to the SSK Insurance System (similar to the U.S. Social Security System) a Smart Card. The Smart Card will be a depository for all transactions as well as other vital contact and medical information for the patient. Information stored on the Smart Card will allow swifter and more accurate transactions and vastly improve the quality of service offered by the national health system.

### 28.2.6 Security assessment tools / Content Screening, Anti-virus and mobile code

Not surprisingly, the only anti-virus measures taken by the majority of PC customers and small / medium enterprises rely on the Norton Anti-virus program. The Norton product, with its 90% share, dominates the market.

### 28.2.7 Data warehousing and information

Data warehousing is available at low costs via most ISPs. Turkish ISPs provide hosting, either with FTP or Front Page extensions, at prices compatible with those of the U.S. In addition, they also provide customers with FTP accounts, which are secure intranet accounts, in a sense accessible only by those within the company, but on a global scale.

Another important data warehousing system developed by Turkish ISPs allows customers to connect their own PCs on the ISP premises, for a fee, allowing the connected PC to work as an online server on behalf of the company. This eliminates the relatively high ISDN lease line costs charged by Turk Telecom yet provides the user with a 24 hour, 7 days a week server into which the company can dial.

### 28.2.8 Internet Security market opportunities

Internet security is not the major IT business trend in Turkey. Although American and Western European firms have long been committed to e-commerce; the true dimensions and impact of the internet are just now hitting the Turkish market. The slower development has been driven by the high costs of development for online shopping and credit card verification. High development costs have reserved e-commerce businesses for the firms with the capital to invest and have precluded the smaller, entrepreneurial companies.

The number one market obstacle to increasing Internet security systems in Turkey rests with the fact that e-commerce has not fully taken off - there is limited need for internet security systems. This is bound to change rapidly with the push from the private sector combined with new initiatives undertaken by the Turkish Government

(GOT). A new GOT Task Force, determined to advance e-commerce, is grappling with issues such as customs, consumer rights, legal aspects, technical policies, as well as administrative and financial issues.

## 28.3 Competitive analysis

Market accessibility depends on selling to key IT players, which are usually the technology firms belonging to the large holding companies. Two examples of such companies are Garanti Technology (providing technical know-how to Garanti Bank, Ottoman Bank, Garanti Insurance etc.) Yapi Kredi Technology (providing know-how to Yapi Kredi Bank, Pamuknank, Superonline, Turkcell, etc.). The companies that build the technology backbones for their Groups are the key decision-makers for the purchase of goods and services.

### 28.3.1 Position and prospects of U.S. companies

A strategic way to enter the market is through an alliance with an existing Turkish solution provider with experience and a business portfolio in building networks for medium and large companies. These companies are at the moment diversifying themselves towards software development, out-sourced technical support, and e-commerce solutions. The internet security business is certainly linked to the development of e-commerce in Turkey.

American companies are still at the top of the list for Turkish IT companies looking to do business. The proliferation of American technology products plus the high compatibility with systems common in Turkey give U.S. IT products an important advantage in the market.

## 28.4 Statistical information

### 28.4.1 Utilization and penetration of the Internet

Number of internet users in 2000 in Turkey: 1.7 million
- estimated by 2001: 3 million
- estimated by 2002: 6 million
- estimated by 2003: 7.5 million
- estimated by 2004: 10 million

Total Turkish Website address sold to date: 26,017 names, as follows:
- com.tr: 20,247
- org.tr: 1,163
- edu.tr: 137
- k12.tr: 239
- bbs.tr: 41
- gov.tr: 610
- net.tr: 137
- mil.tr: 6

- gen.tr: 3,249
- nom.tr: 188

Source: Middle Eastern Technical University.

Top market shares of ISP's:
- Superonline: %50.7
- Turk Net: %10.4
- Vestel Net: % 8.8
- Ixir Net: %5.0
- Kocnet: %4.4

Age Profile of internet users in Turkey:
- Ages 10-20: 6%
- Ages 20-30: 58%
- Ages 30-40: 24%
- Ages 40-50: 5%
- Ages 51 and up: 1%
- Other: 6%

Most popular products sold via e-commerce in Turkey
- Books: 36%
- CD / Cassette / DVD: 32%
- PC Products: 16%
- Clothes: 14%
- Electronic Goods: 14%
- Food: 14%

### 28.5 Contact information

US Commercial Service Turkey
Ihsan G. Muderrisoglu
Ataturk Bulvari No. 110
K.Dere, Ankara, Turkey
Tel: [90] (312) 467-0949
Fax: [90] (312

# 29 United Kingdom

# 30 Ukraine

### 30.1 Summary

The Ukrainian Internet sector is still too small and underdeveloped to focus on Internet security or related issues. Due to its limited development, even the industry in Ukraine has only a vague idea of security issues related to its development.

Nevertheless, the Ukrainian Government (GOU) seems more interested in Internet security than in encouraging the development of Internet business. The Ukrainian Government, in short appears intent and determined to regulate what little exists or may exist in the future.

Current GOU legislation lacks provisions to protect Internet businesses. To date, no national plan or design, for monitoring Internet traffic exists. Though monitoring of the Internet, to prevent the distribution of personally offensive or dangerous information, is often used as the reason for advocating an overall control of Internet content.

Economic factors in Ukraine, such as the weak business environment for small and medium size companies, the low income of Ukrainians, and the limited number of Ukrainians using computers on a daily basis, restricts the growth of the Internet. The lack of legislation, which would outline the legal status of Internet-related businesses (e.g. Internet telephony, e-commerce, and information security, etc.) also poses major obstacles for the development of Internet related businesses in Ukraine. On the other hand, substantial changes and improvements for foreign investors have occurred in the Ukrainian telecommunications legislation as of July - August 2000. The legislation now permits and encourages foreign companies to operate in the Ukrainian telecom industry on an equal footing with Ukrainian companies.

## 30.2 Market Overview

### 30.2.1 Internet

The Ukrainian telecommunications market is young and limited in size. The income level of the Ukrainian population and the number of Ukrainians using computers on a daily basis are determining the rate of development of the Internet. Another factor influencing Internet growth, is the degree of business integration into Western markets. Differing from the U.S. and Western Europe, the Ukrainian Internet market, depends more on the availability of telephone communications and the computer infrastructure than the need for Internet Service Provider (ISP) services. This dependence is due, to a large part, on the monopoly of Ukrtelecom in the public telephone system, the last mile “problem” and charges to access international channels.

Identified obstacles (by the industry) for the development of additional Internet services are:

a) The lack of a local loop development
b) Legislation that would determine the legal status of Internet-related businesses (e.g. Internet telephony, e-commerce, and information security.)

A additional technical difficulty faced by Ukrainian ISPs, is the lack of developed Ukrainian wireline network:

a) Only 20% of the Ukrainian local telephone exchanges are digital,
b) Only 5,000 out of 130,000 phone channels are fiber optic (Kompanyon No. 24, June 2000).

c) The last mile "problem" is a nightmare for all ISPs. Even, in Kiev some phone exchanges are unable to provide a reliable connection for an on-line Internet access near the end of an exchange.

Before December 1997, Internet Service Providers (ISP) were subject to licensing. There were 103 companies identified with the business: -- 22 firms were located in Kiev, 13 in Donetsk and 10 in Dnypropetryvsk-- (Source "Byznes" No.26, June 1998). The cancellation of mandatory licensing stimulated the growth in the number of ISPs. Based on official statistics, there are now approximately 260 ISPs in Ukraine--seventy are located in Kiev--. (Source: Kompanyon No. 24, June 2000). The industry believes that 30 to 40 of the leading ISPs, that have experience, size and finances, determine the development of the national market. The remaining --220+-- ISPs are either, small peripheral operators or in a short-term business.

The following ISPs, are the leaders of the industry in the Ukrainian market:

- Lucky Net,
- Infocom,
- Ukrtelecom,
- UkrSat,
- Global Ukraine,
- IP Telecom,
- Golden Telecom Business Solutions,
- Monolit,
- Relcom Ukraine, etc.

In 1998 the demand for ISP services in Ukraine slowed: e.g. in 1996-1997 both the number of international Internet channels and the number of customers increased by a thousand percent, but in 1998 these numbers only doubled. In 1999 ISPs reported a 300% increase in revenues. Official GOU sources estimate that Ukrainian ISPs reached 400% profitability levels in 1999 (Source: Kompanyon No. 24, June 2000). Industry sources disagree with the estimates, ISP services in 1999, and sales estimates ranged from $15 million to $60 million, but industry sales appear to be closer to $20 million. The analysis of revenues received by ISPs, indicate that 99% of the revenues are generated by payments for Internet access, while web design and hosting, provided for less than 1% of industry revenues. ISP still remains the core business in this industry. Businesses, such as e-commerce, web design and hosting are in most cases developed by successful ISPs as a side business in anticipation of future income. There are no official statistics for the number of Internet users in Ukraine. By unofficial count there are approximately 600,000 Internet users in Ukraine, or 1.1 percent of population. Most Ukrainian users of the Internet live in Kiev. Though numbers of Internet customers increased by 25% in 2000 there is a limit to this growth, imposed by the number of PCs available in Ukraine. There are approximately 1 million PCs in Ukraine and only 40% of them are adaptable for Internet access. It is a reason, why most ISPs focus on creating collective Internet centers at universities, colleges, Internet cafes, etc.

The ISPs that seriously focused on young Ukrainians, as a future customer base, launched a prepaid web card in 2000. Currently, 10 ISPs offer a prepaid web card. Managers of these firms expect that the reduced cost of the service will expand their customer base. The cards allow customers to save on monthly and registration fees

by offering lower rates. The service offer is expected to attract customers who cannot afford or do not need regular Internet access.

Presently, the ISP sector is regarded as low in profitability; the need to reinvest reaches 95 percent. However, this sector seems to be performing better than other ICT industries, mainly due to active domestic and international investments. On April 27, 2000, investment bank Wood & Company (www.wood.com) announced allocation of $ 50-70 million to create an isolated investment fund. The fund aims at financing I.T. and Internet projects in Ukraine. The fund is focusing on 20-25 I.T. and Internet service projects with investments ranging from $ 50 thousand to $ 5 million. The investor/bank intends to retain a minority share in companies implementing such projects. These shares will then be put on sale through an auction in 2-5 years.

In December of 1999 three Ukrainian I.T., Firms Quazar-Micro Radio, IP Telecom and Relcom Ukraine formed an I.T. holding company called the "Nadyma Group". This holding company focused on attracting "portfolio" investors for a number of new projects. The identified investors, Societe Generale Landenburg Thalmann (SGLT), now control the Nadyma Group, who planes to trade its shares on the European and New York Stock Exchanges.

The investments by an international investment fund represent a substantial support to the Ukrainian I.T. and the ISP industry. To launch an ISP business in Ukraine requires no more than $ 200,000-500,000 however, if the ISP desires to expand in the network, and be competitive, a more substantial outside investment is required. This need, is a problem in a country with very high interest rates and an almost nonexistent stock market.

To expand the local market for Internet services and reduce the demand on international connections, ISPs have created the "Ukrainian backbone network". ISP companies that operate outside of Kiev are at a disadvantage, because they have to pay for access to an international channel and lease fiber optic lines from their region to the capital (similar in costs to international access). To reduce these costs, regional providers use radio relay channels that are outdated and unreliable, or voice band frequencies of Ukrtelecom. In the near future regional ISPs may opt for satellite channels. It is a fact, that many larger ISP providers feel the need for additional Internet connectivity. Substantial growth in Internet traffic and the expensive of international channels has forced ISPs to look for affordable Internet connections through satellite access. This need also represents a " best sales" prospect for U.S. companies.

Ukrkosmos, a leading satellite provider, is using the site and ground infrastructure at the old Inmarsat station located near Odessa to install an Intelsat antenna to transmit Internet traffic through the Intersputnik satellite. In the meantime, all Internet traffic originated by Ukrkosmos customers is transmitted by an up-link station in the Kiev City TV tower to the LMI-1 satellite. Ukrkosmos is one of three companies (along with Infocom and Ukrtelecom) that have been granted the privilege to provide Internet service to those Ukrainian State entities that deal with sensitive and classified information.

ISPs often use satellites in conjunction with fiber optic channels to reduce the costs of international connections. For instance, Infocom, one of the largest ISP in Ukraine with subsidiaries in 120 cities and towns, offers a dial up and dedicated connection to a 4Mbit/s link of the Internet backbone, including direct connection to Teleglobe International. Infocom is offering Internet access by a satellite channel with a capacity of 45 Mbit/s via an asymmetric solution: four satellite dishes located in regional centers and Kiev receive satellite data. Outgoing data is transmitted via fiber optic channels leased from Ukrtelecom. Infocom has found this structure the most cost effective, allowing it to save on frequency license and frequency fees.

### 30.2.2 Commerce, Internet Banking, Mobile Internet

E-commerce is gaining in popularity in Ukraine despite the lack of a credit card payment system (Ukrainian banks issue only debit cards), the limited number of international credit card holders, and the lack of Ukrainian legislation containing provisions for the use of internet, e-commerce, or an electronic signature. It is surprising, but the numbers of virtual stores are constantly on the rise. Their numeric growth rate is far ahead of the growth in number of customers that use this service. However, it should be noted, that most Ukrainian Internet shops are price lists with an option to place an order, that later could be delivered, after a cash payment or bank transfer is received. Only a couple of Internet shops accept on-line payments from clients or their partner- banks.

Some Ukrainian Government officials, though purporting to understand the benefits of e-commerce, believe that e-commerce should be limited in Ukraine until Ukrainian businesses are ready to participate in it. Otherwise, these officials believe, foreign products marketed via e-commerce will dominate the market.

Another perspective, is that there is no point in discussing e-commerce in a country where only 0.5% of population have access to Internet and only 2% have credit cards. But both businesses and customers view e-commerce in Ukraine more as entertainment than a serious business opportunity. A psychological mistrust seems the main obstacle for a business to customer e-commerce relationship in this country. However, business to business e-commerce in Ukraine has experienced a successful start, in such areas as, metals trading, I.T., and transport services. Trading in grain commodities may also be a very promising subsector for business to business e-commerce.

Many Ukrainian banks offer PC banking. The customers of PC banking are corporate clients. The limited number of corporate clients that need this service and the cost associated with a client-server application, limits the use of this service. Internet and mobile banking, currently offered in Ukraine is limited to obtaining information, about the status and movement of funds in bank accounts, through the internet or mobile phones. Bank clients cannot implement transactions through the Internet or by mobile phones due to the prohibitive regulations in this sphere.

It is puzzling, but the National Bank seems more concerned about the security of transactions made through Internet and mobile banking than about the availability of the service. They have attempted to regulate what does not even exist yet. In the other extreme, some Ukrainian banks have started to offer their clients Internet

banking in anticipation, of expected changes in the regulatory environment. They have also partnered with leading mobile telecom providers in offering mobile banking as a value-added service, to enhance the provider's competitiveness. In a country with limited integration into the electronic world, the prospects of virtual services, is an indication of a desire to join the world of modern technology.

A recent incentive offered by MC operators is mobile Internet. In May of 2000 Kiev Star, a leading MC operator, started offering mobile Internet services based on a Wireless Application Protocol (WAP). The service provides customers with access to news, currency exchange rates, weather forecasts, etc. In the future, the company plans to include an Internet service package access to e-mail, e-commerce, Internet banking, and a log-on to a corporate network. This project establishes a link between two of the most dynamic sectors of the Ukrainian I.T. and telecom markets. This service offers an opportunity to U.S. exporters of technology and solutions for the mobile Internet.

### 30.2.3 End-User Analysis

Research conducted in Kyiv by the Marketing & Media Index Company in early 2000 indicated that: 50% of Kyiv citizenry use a PC.

a. 30% of the population are office PC users,
b. 15% use PCs at home,
c. 8% use PCs in school, college or university,
d. 6% use PCs in other public facilities such as an Internet cafe, library, etc.

Approximately 226,000 of Kyiv citizens use e-mail. Around 255,000 people in Kyiv access Internet at least once a month, while 87,000 use Internet on a daily basis.

a. 24% of the Internet users access it from home,
b. 58% use the office,
c. 16 % access Internet from other public facilities such as Internet cafe, etc.
d. 9% access internet from college, school, or the university.

Approximately 23% of internet users visit e-commerce sites when looking for consumer goods, however, only 2% made a web purchase during the last six months (Source: Kompanyon No. 24, June 2000).

### 30.2.4 Internet Security

Internet security is a concept that is interpreted differently by different aspects of the Ukrainian IT markets. Due to a lack of development in the Ukrainian internet related businesses and the basic services provided by ISPs, even industry insiders have only a vague idea of security issues related to the internet. They refer to security specialists working for law enforcement and security agencies, when dealing with the subject.

On the other hand, representatives of Ukrainian law enforcement agencies understand security, but do not have experience in applying it to the Internet.

Ukrainian government officials associate Internet security with national security in the ICT sphere. They believe that the government through security agencies should control the Internet, by monitoring Internet traffic and Internet licensing. The difficulty lies with the Ukrainian government having neither financial resources nor qualified staff to implement such a control. That is why government officials opened a dialog with ISP companies, and has attempted to implement traffic monitoring at the companies' expense. In this regard, licensing ISP businesses can be regarded as a leverage to influence ISPs to cooperate with the government on security issues. Though some of the biggest ISPs welcome licensing (mainly because they have paid for licenses before 1997 and expect that bureaucracy and the additional expenses related to licensing, will destroy competitors). Many ISPs view licensing as an additional obstacle and will tolerate it as an inevitable evil if mandated. Most ISPs however are not ready to pay for government security initiatives; they are concerned with keeping up with the ever-changing market and the competition.

Discussions between security related Government of Ukraine (GOU) agencies and ISPs focuses on the following related topics to Internet security:

- Legislative norms for the developing Internet in Ukraine (e.g. laws "On national strategy in developing and using Internet resources'", "On the protection of information in ICT networks", "On electronic documents", "On electronic signature", "On protection of private information")
- Informational security (including the monitoring and control of illegal information)
- Protection of data transferred via I.T. networks, and the protection of state information or information under state control
- The legal monitoring of data transfer networks is possible only if implemented according to national and international laws, including resolutions of Counsel of Europe ENFOPOL 98
- Organization and technical perspectives of Internet addresses using the domain "ua"
- The national domain "ua" needs to be administered by a company/agency resident in Ukraine

Problems for Internet security in Ukraine lie in the legislative arena. Current Ukrainian legislation lacks all provisions necessary to conduct business via Internet. At least five laws (e.g. "On national strategy in developing and using Internet resources'", "On protection of information in ICT networks", "On electronic documents", "On electronic signature", "On protection of private information") need to be adopted to provide the minimal legal protection for Internet businesses and end-users. The industry specialists believe that a chapter dedicated to computer crimes needs to be added to the Criminal Code of Ukraine. An alternative opinion is that special laws are not needed only amendments to existing legislative act.

Based on current Ukrainian legislation, any contract or financial transaction conducted via Internet will be considered legal only, after hard copies of the documents are signed, stamped and registered. Taxation in Ukraine is implemented only on a hard copy document.

Administration of the national domain "ua" is also a problem. Currently a non-resident of Ukraine administers this domain. The GOU is eager to administer and develop this domain, but has neither funding nor staff to accomplish it.

Ukrainian banks have concerns in regard to security of Internet transactions. Late in 2000, the National Bank of Ukraine attempted to secure e-business by preparing a draft regulation on the subject. The intention of the document was to regulate the operation of the electronic shops, placement of orders, control of electronic payments with debit/credit cards and maintain a "bank-client" relationship. Most importantly, the draft was to oversee the development of a national system for the use of an electronic signature for on-line transactions. The draft regulation insisted on the electronic authentication of both customer and seller (Source: Compass, October-November, 2000).

Protection of public, corporate and private networks against attacks by computer hackers and viruses is also a matter of concern for the GOU and ISPs. As GOU agencies join the Internet, the possibility that corporate GOU networks may become victims to Internet attacks becomes real. While Security for the GOU is entrusted to specialized GOU agencies, most banks, corporations and ISPs solve problems on their own. However, little attention is being paid to the individual end-user.

There is no national system for monitoring Internet traffic, to prevent distribution of offensive, racially dangerous, sexual, religious or other objectionable content, though concerns of this kind exist and is often used for advocating the control of the Internet.
As mentioned above, Ukrainian legislation lacks provisions necessary to regulate the use of ICT hard and software. This is also true for cryptographic hard and software. There are norms that would prohibit downloading of cryptographic software from the Internet for use in private or corporate networks. However, anyone planning to use cryptographic equipment or software on a public network needs to certify the products and obtain a license for its importation. A license to import cryptographic equipment is issued to Ukrainian companies only.

IPR legislation exists in Ukraine and though it has many loop holes, its weakness lies in the enforcement of IPR issues. This weak protection and enforcement of IPR in Ukraine has a negative impact on the computer software and audio/video products market. It is therefore difficult to expect IPR legislation in Ukraine to protect products marketed via the Internet. Companies should recognize this fact and consider it when doing business in Ukraine.

The Ukrainian Internet market is currently too small and underdeveloped to feel an impact from security related factors. Ukrainian authorities, however, seem concerned with Internet security and are trying to regulate its development.

### 30.3 Statistical Information

STATUS AND POTENTIAL OF UKRAINIAN ICT MARKET

| Local market of ICT Products and Services | Customer Base (Compared To The Population Of Ukraine) | Industry Revenues |
|---|---|---|

| Products and Services | Population Of Ukraine) | |
|---|---|---|
| Current | 3% | $ 3 Billion |
| Potential | 25% | $25 Billion |

(Source: Speech by Mr. Oleh Shevchuck, Head of the State Committee for Communications of Ukraine, at American Chamber of Commerce meeting in Nov. 2000)

DEVELOPMENT OF INTERNET IN UKRAINE

| | 1997 | 1998 | 1999 | MAY 2000 |
|---|---|---|---|---|
| Number of Internet users | 20,000 - 25,000 | 110,000-120,000 | 150,000-300,000 | 150,000-230,000 |
| Number of web sites with domain "ua" | | | | 7,500 – 11,000 |
| Number of ISPs | 105 | 158 | 200/207 | 260 |

(Source: Kompanyon No. 24, June 2000).

REGIONAL MARKETS OF INTERNET SERVICES

(As of June 1999-May 2000)

| CITY / REGION | NUMBER OF CUSTOMERS | NUMBER OF ISPs |
|---|---|---|
| Ukraine total | 100% | 260 |
| Kyiv | 30-45% | 39-67 |
| Kharkyv | 10% | 9 |
| Donetsk | 8% | 11 |
| Odessa | 4% | 12 |
| Lvyv | 3% | 6 |
| Dnypropetryvsk | n/a | 14 |
| Zaporyzhzha | n/a | 9 |

(Source: Kompanyon No. 24, June 2000)

ISP MARKET IN KIEV

| | APRIL 1999 | APRIL 2000 |
|---|---|---|
| Number of ISPs | > 43 | 60-67 |
| Total capacity available in Kyiv for international connectivity | 17.1 Mb/sec | 92.51 Mb/sec |

| | | |
|---|---|---|
| Total capacity available in Ukraine for international connectivity | 19.2 Mb/sec | 92.51 Mb/sec |
| Total number of telephone channels used for ISP in Kyiv | > 1698 | > 3168 |

(Source: Kompanyon No. 24, June 2000)

REGISETRED WEB SITES BY REGION

(As of March 2000)

| REGION | NUMBER OF REGISTERED WEB SITES | SHARE OF THE TOTAL NUMBER OF WEB SITES |
|---|---|---|
| KYIV | 2876 | 45% |
| OTHER REGIONS | 3423 | 55% |
| ODESSA | 879 | 14% |
| DNYPROPETRYVSK | 441 | 7% |
| KHARKYV | 434 | 7% |
| DONETSK | 280 | 4% |
| LVYV | 198 | 3% |
| CRIMEA | 155 | >2% |
| ZAPORYZHZHA | 127 | 2% |
| CHERNYHYV | 106 | 1.5% |
| OTHER | < 100 | 12% |

(Source: Kompanyon No. 24, June 2000)

## 30.4 Overview of ICT Market Infrastructure

### 30.4.1 Computers & Peripherals

The size and make up of the Ukrainian computer hardware market is difficult to measure, since official statistics ignore such key factors as local production, and the "shadow" importation of components. Local production based on imported components is thriving and reshaping the structure of the market.

Based on data provided by the market, the importation of brand name computer equipment decreases 10 percent annually, and the importation non brand name equipment is less by 15 percent each year. This phenomenon is attributable to the taxation of imported PCs versus imported components. At the same time, the demand

for locally manufactured computer hardware (i.e. from imported components) is steadily increasing. Local assembly is expected to reach 75 percent of the total market in 2000. Of the nearly 700 companies involved in PCs and active in the market, approximately 66 of them are engaged in the assembly of PCs. Eighty percent of these computers are Intel based. The industry estimate that only 10-15 percent of Ukraine's potential computer hardware demand has been tapped. The problem lies in the lack of purchasing power of the consumers, a situation, which is not likely to improve soon. The industry estimates that there are approximately 1 million PCs in Ukraine.

Major U.S. computer manufacturers have strong brand-name recognition, but price has proven to be the key consideration for the Ukrainian buyer. Local companies sell between 10,000 to 20,000 PCs annually. Although increasing, home use of PCs is still very limited. U.S. companies may maximize export potential by tapping into an increasingly sophisticated network of agents and distributors throughout Ukraine. These agents are able to reach a wider range of clients and are familiar with the customer base.

Tangible trade opportunities lay in the telecommunications and transport segments as well as in the regional and city administration levels.

### 30.4.2 Computer Software & Services

Ukraine's expanding private sector requires diverse software solutions and packages. However, the poor enforcement of intellectual property rights in Ukraine is a factor to be noted by U.S. companies interested in entering the market. Early in 2000 Ukraine was identified as a center for the illegal manufacture of audio and computer discs. These manufacturers produce up to 36 million disks annually, with an internal demand not exceeding 5 million. At the request of international copyright protection associations and the United States Government, Ukrainian authorities have closed some manufacturing sites in June of 2000.

Microsoft's Office and Windows programs are currently the most widely used office software in Ukraine. This software is installed on approximately 98% of all PCs operating in the country. The presence of many talented programmers, combined with a weak International Property Rights (IPR) legislation and enforcement, has encouraged piracy and flagrant misuse of software. It is estimated that illegal software may account for 10 to 40% of the software used by the government, 10 to 30% used by corporate customers, and 50 to100% used by small and medium businesses and home users of PCs. Foreign software dominates the market for legitimate software use for corporate customers, reaching 95%; local products do not exceed 5%. A more legitimate and transparent market for computer software is slowly taking shape. This change is largely attributed to dealers selling hardware with preinstalled, legally acquired software.

Ukraine has witnessed an increasing demand for specialized financial, statistical, management, and manufacturing software. These demands present viable opportunities for U.S. companies. For maximum market exposure and penetration, U.S. companies are urged to develop bilingual (Ukrainian/Russian and English) software, as well as to provide the necessary bilingual written instructions and after-

sales service. The existing legal environment in Ukraine does not include many important specifics that would regulate the localization of software products. Legitimate localization of foreign software products is almost non-existent, which is partially due to competition from products localized in Russia.

Ukraine is slowly emerging as a low cost site for qualified software development. The producers, work mostly alone or in small groups on projects ordered from abroad. This activity is usually not reflected in official statistics. There is a growing interest in Ukrainian computer companies to organize software production centers that could participate in international software development projects. However, the level of emigration among qualified programmers and the controversial Ukrainian legislation, delay development of software techno-parks in Ukraine.

### 30.4.3 Telecommunications

#### *30.4.3.1 Wireline Communications*

Advances in wire-line communication includes the completion of a national telecom network with 45 long-distance exchanges (27 are digital and located in regional centers; the other 18 regional exchanges are analog), and 3 digital international gateways. Ukraine has installed a national fiber optics network connected to international fiber optic systems: ITUR, TEL, TAE, and BSFOCS. The fiber optic network consists of 4,200 km of fiber and digital microwave communication lines. Currently, this network is expanding toward neighboring regions of Russia. Ukrainian users now have available international telephone connections to more than 200 countries. The average teledensity is 19.8 telephones per 100 inhabitants. The annual per capita spending for telecom services in Ukraine is $20.6 (Source: Telecom, No. 10, October 1999)

Two companies dominate the national and long-distance wire line networks: Ukrtelecom and Utel. There are a number of other providers of wireline services (e.g. Golden Telecom Business Solutions, Kancom/Andrew, Optima, Farlep, Lyuza, Intersvyaz, Crymtel, and Telecominvest) but their total number of customers does not exceed 120,000, thereby making their share of the local market insignificant.

Ukrtelecom was created in 1993, when the Ukrainian Ministry of Communications reorganized the national telecommunications structure by merging several telecom departments and regional PTTs into the Ukrainian State Telecommunications Corporation (Ukrtelecom). Owning all transmission facilities, Ukrtelecom administers the national wire line infrastructure. The company employs more than 130,000 people.

Ukrtelecom's revenues in 1999 reached $ 627 million, a 30% increase when compared to 1997, if calculated in local currency, but 50% lower if calculated in $. The reason given, is because the Government of Ukraine (GOU) who regulates Ukrtelecom's rates, has not modified them in over a year and a half. New rates were approved early in 2000.

Plans to privatize Ukrtelecom have been repeatedly announced since 1997-1999, but fierce opposition delayed privatization. The law on privatization of Ukrtelecom was

adopted on July 13th, 2000. Privatization, when it does occur, is expected to reshuffle the telecom industry in Ukraine.

The long-distance and international provider Utel (currently owned by: Ukrtelecom 70.5 percent, Deutsche Telecom 19.5 percent, Brokbusiness Bank 10 percent) was created in 1992. Utel owns two out of three international gateways available in Ukraine and controls more than 90 percent of the international traffic. With 1,700 employees and 23 affiliate offices, Utel has enjoyed success: Utel's total revenues exceeded $338 million in 1998, with a profit of $38 million. The company's performance in 1999 was impacted by the financial crisis: Utel's total revenues in 1999 were only $255 million, with a profit of just $ 14.6 million.

Ukraine's wire line network is far from optimal. Fees for line installation can reach $ 1000, and installation may require a substantial wait. Although an increasing amount of digital equipment is in place, many regional switches continue to connect customers through outdated equipment. Out of the 10 million phone lines, only 10% are serviced by digital exchanges, another 10% are supported by electronic and quasielectronic exchanges. Obsolete relay and mechanical equipment service the rest. This limits the introduction of a new electronic billing system. Most users now pay a symbolic fee of $ 2-3 per month. Only in urban areas has the new billing system, based on per minute use, been introduced.

In small towns and villages, the situation is even worse. There are instances where only one line exists in a village of several thousand people; the wait for a line can range from 7 to 11 years. To date, almost all-rural local loops are unprofitable. Ukrtelecom subsidizes local loops with revenues from inflated fees for international calls, line installation, and registration. The number of phone lines may vary throughout a region. Kiev has the highest teledensity (43.6 percent), followed by the industrial regions in the east (19 percent). Telephone lines are relatively rare in the agricultural regions of Transcarpathia and Carpathia, located in the western part of the country. Estimates indicate 3.3 million people are on the waiting list for individual phones. At the same time, there is an excess of 800,000 available telephone connections. Ukrainian customers cannot afford to pay $300 to $1000 for installation. As stated earlier, Ukraine's telecommunications infrastructure has developed significantly since 1992, but still lags behind Eastern and Central European countries. The Government of Ukraine (GOU) hopes to raise average wireline connections from 19 to 40 percent of the population over the next 10 years, approaching western standards. This will require the installation of 10 million new phones, which would cost from $ 5 to 10 billion. These calculations require a $ 1 billion annual investment into the industry, which only seems feasible if Ukrtelecom is privatized and the Ukrainian economy improves. In the meantime, wireless communication is emerging as the most viable alternative for corporate and business clients.

### *30.4.3.2 Wireless Communications*

Wireless mobile communication is currently the most active subsector of the telecom industry in Ukraine. Market penetration for mobile communication (MC) is 1.5 percent only, but the number of customers doubles each year. It is a promising sub-sector, because of the investments it has received since 1997, when the GSM900 network was initiated. Mobile service customers number no more than 600,000 (as

of November 2000), but significant discounts in fees and the introduction of flexible payment plans are increasing these numbers dramatically.

The most striking feature of the Ukrainian mobile Communications market is the number of operators. Five operators offer wireless mobile services in the following standards: GSM900 (operators: UMC, Kiev Star, Welcom), NMTi 450 (operator: UMC), DCS 1800 (operator: Golden Telecom GSM), and D-AMPS (operator: DCC). Three more operators: Ukrainian Wave, Telesystems of Ukraine, and ITC are deploying CDMA and TDMA wireless local loop networks with a potential to go into mobile.

An advantage for MC operators is that they don't have to adhere to the artificially low telecom rates established by the GOU. But since their only access to the local loop is through Ukrtelecom, and there are more MC operators than the market can support, they are very vulnerable to decisions made by GOU agencies and Ukrtelecom management. With high rates for GSM900 spectrum frequencies, a limited number of customers and the existing number of operators, the competition in the Mobile Communications market is harder every day. However, recent investments into the MC sector by EBRD, international telecom equipment manufacturers and service providers, indicate that some market players are optimistic and ready to invest on future dividends.

In the mean time, the market has started to consolidate around two major operators: UMC (Ukrainian Mobile Communications) and Kiev Star. The number of UMC customers reached 285,000 in September of 2000 (compared to 186,000 in March of 2000), and Kiev Star users have more than tripled in the same period and exceed 185,000 individuals as of September 2000. Industry insiders speculate that at least two of the remaining Mobile Communication (MC) operators are considering selling their networks, which will further consolidate the market. If the MC market / or user base continues to grow at the same rate, the number of MC users in Ukraine may reach 750,000 by the end of 2000. These numbers are impressive, when compared to 1998, when there were only 186,000 MC customers and 320,000 in 1999. Prepaid MC services, mobile banking, mobile Internet, SMS and other value-added services have allowed MC operators to attract customers from other telecom sectors, such as paging and trunking.

## 30.5 Contact Information

### 30.5.1 AMERICAN EMBASSY

Commercial Service
7, Kudriavsky Uzviz, 2nd Floor, Kyiv 252053, Ukraine
Tel: (380-44) 417-2669, 417-1413; Fax: (380-44) 417-1419
Contacts: David Hunter, Senior Commercial Officer
Bela Babus, Commercial Officer
Ruben Beliaev, Industry Commercial Specialist

### 30.5.2 UKRAINIAN GOVERNMENT

1) State Committee for Communications and Information Technologies of Ukraine

(Formerly the Ministry of Communications of Ukraine)
22, Khreshchatyk, Kyiv 252001, Ukraine
Tel: (380-44) 226-2140; Fax: (380-44) 226-2926
Contact: Oleg Shevchuck, Head

2) National Space Agency of Ukraine
11, Bozhenko St., Kyiv 252022, Ukraine
Tel: (380-44) 226-2555; Fax: (380-44) 269-5058
Contact: Olexandr Nehoda, Director General

Tel: (380-44) 268-7218; Fax: (380-44) 269-5058
Contact: Mr. Eduard Kuznetsov, Deputy Director for Satellite Communications

30.5.3 Major Telecom Operators and ISP

1. Kiev City ISP Portal providing info about all ISPs located in Kyiv
http://providers.org.ua

2. Digital Cellular Communications (DCC)
36/1, Melnykova St., Kiev 252119, Ukraine
Tel/fax: (380-44) 246-9092
Contact: Olexander Ivanovich Fedorov, Country Director

Operator of D-AMPS mobile cellular phone services
3. Elsacom-Ukraine
1, Phyzkulturna St., 4th Fl., Suite 416, Kyiv Ukraine
Tel: (38044) 246-6317/466-1071; Fax: (38044) 227-5524/466-1067
Contact: Kirill Kozlov, Director General

Representative of Globalstar in Ukraine
4. Global Ukraine
27, Panasa Myrnoho St., Kyiv 252011, Ukraine
Tel/Fax: (380-44) 294-4366/67
Contact: Yuriy Korzh, Director General
www.gu.net

ISP
5. Golden Telecom GSM
14/1, Mechnykova, Kyiv 252023, Ukraine
Tel: (380-44) 247-5683; Fax: (380-44) 247-5670
Contact: Jeff Howley, Director
www.goldentele.com

Provider of DCS1800 cellular telecommunication services,
Fiber optic business lines, ISP

6. Infocom
10, Volodymyrska St., Kyiv 254025, Ukraine
Tel: (380-44) 212-2234; Fax: (380-44) 228-7340
www.infocom.com.ua

Contact: Vasiliy Polischuck, Director General

ISP and satellite services
7. IP Telecom
34, Lesy Ukraynky Blvd., Suite 213, Kyiv Ukraine
Tel/Fax: (380-44) 238-8989; 295-5514
E-mail: mail@iptelecom.net.ua
http:\\www.iptelecom.net.ua

ISP
8. Kiev Star
51, Krasnozoryanyy Prospect, 2nd floor
Kyiv 252110, Ukraine
Tel: (380-44) 247-3910; Fax: (380-44) 245-7208
Contact: Ihor lytovchenko, Director General

Operator of GSM900 mobile cellular network
9. Link Telecom Ukraine
57/3, Krasnoarmeyskaya St., Kyiv 252150 Ukraine
Tel.: (38044) 461-9222; Tel/Fax: (38044) 461-9223
http\\www.link.com.ua

Paging
10. Lucky Net
19/7, Lypskaya St., Suite 49
Tel/Fax: (380-44) 238-8823
e-mail: azarov@lucky.net
www.lucky.net
Contact: Sergiy Azarov, Director for International Relations

ISP
11. Monolit
1/27, Lykhachova St., Kyiv 252133 Ukraine
Tel: (380-44) 295-9080; Fax: (380-44) 295-3053
Contact: N.A. Bakanov, Director General
htpp:// www.ua.net

ISP
12. Ukrainian mobile communications (UMC)
40, Gorky Str.,
Kyiv, Ukraine 252005
Tel. (380-50) 310-0010; 220-42-37
Fax. (380-44) 290-5351

Major operator of GSM900 and NMT4 mobile telecommunication services.
13. Ukrkosmos
37, Pobedy Ave., Bld. 28, Kyiv Ukraine
Tel: (38044) 241-8472, 241-8473
www.ukrkosmos.kiev.ua
Contact: Mr. Alexander Makarov, Director

14. UkrSat
12, Borysoglebska St., Kyiv Ukraine
Tel: (38044) 238-2555/ 238-2599; Fax: (38044) 238-2566
E-mail: market@ukrsat.com
www.ukrsat.com
Contact: Mr. Vladymyr Loman, Director General

15. Ukrtelecom
18, T. Shevchenko, Kyiv 252030, Ukraine
Tel: (380-44) 225-3254; Fax: (380-44) 229-8593
Contact: Satnyslav Dovhiy, Director General
http://www.ukrtel.net

This state owned corporation controls all the national wire telecommunications including basic networks, data transmission channels.

16. Utel
34, Bohdan Khmelnitskiy St., Kyiv 252030, Ukraine
Tel: (380-44) 229-8622; 220-7100, 229-0864, 229-1265; Fax: (380-44) 229-8373
Contact: Olexiy Marinchuck, President

Major provider of international and long-distance telecommunication services.

# 31 Uzbekistan

**31.1 Summary**

Based on IDC research, the worldwide market for Internet security software increased 32 per cent, from USD 3 Billion to USD 3.98 Billion (1998-1999). Within the Internet security software area, the following four individual markets showed a significant growth in the comparative year growth rates:

· Firewalls (software only) grew 25 per cent.
· Encryption software rose 33 per cent.
· Anti-virus software grew 21 per cent.
· Security authentication, authorization, and administration revenue outperformed all the security markets and grew 41 per cent.

Uzbekistan, a major Central Asian cultural and economic hub, has gone through a rapid wave of changes in the telecommunication and information technologies arena. The past two years produced a sharp rise in the number of users throughout the Republic. According to local estimates the number of users have grown exponentially: there are 10,000 – 15,000 registered users, and about 75,000 users, who have access to the Internet. The number of Internet Service Providers (ISP) reached 39 in this same timeframe. Local experts expect the number of domestic

Internet users to grow steadily over the next few years, exceeding the rate of growth for GNP.

There are several e-commerce projects created by local enterprises, which are awaiting legislation to immediately offer on-line services. Three existing web-shops which operate on cash-on-carry basis and a number of larger e-commerce initiatives, which are be carried out to prepare local users for the new technology era.

The Internet security market in Uzbekistan is still in its initial stage. Due to economic difficulties, deficiency of existing e-commerce ventures, lack of a country-wide credit cards system, only large banks, enterprises and government agencies can afford and justify the installation of very expensive Internet security hardware and software solutions. The other pertinent reason is that most of the domestic enterprises do not have sufficient and substantial information that is open to the web-world.

ISPs, large international corporations, significant local companies, diplomatic entities and some non-governmental organizations are among the few establishments, which invest in Internet security systems. Coca-Cola, Uzbek British American Tobacco, and Zaravshan Newmont Mining Factory have installed and utilize their own Intranets systems. Most popular network equipment producers are CISCO, Sun Microsystems, Siemens, and NEC.

**31.2 Market overview**

The Uzbekistan Internet Services market has a significant growth potential. The past two years brought a sharp rise in the number of users in heavily populated, major economic and cultural central Asian hub, such as Uzbekistan. According to local estimates the number of users has grown exponentially: there are 10,000 – 15,000 registered users, and about 75,000 users, who have access to the Internet. There are 39 Internet Service Providers (ISP). Local experts expect the number of domestic Internet users to grow steadily within the next few years surpassing the rate of GNP. Uzbek companies are slowly utilizing Internet services showcasing their information on the web, and are reviewing the possibility of further expansion into e-commerce, web advertising and marketing, once the opportunity avails itself. Over 1,000 local web sites are registered on the worldwide web-network. More than 30 per cent of them belong to state and non-commercial organizations, 45 per cent are commercial sites, 10 percent are information sites and 15 per cent are entertainment or other sites.

E-commerce projects created by local enterprises, which are awaiting legislation are: zeppelin.uz, ippoex.com and esezam.com. Three existing web-shops which operate on cash-on-carry basis, and a number of larger e-commerce initiatives are carried out to prepare local users for the new technology era. Most of e-commerce initiators explain that their idea is to create an environment for the future users as well as ensuring their niche in this prosperous market.

According to Uzreport.com review, 71 per cent of Tashkent business executives and heads of private companies receive the bulk of their economic information (stock exchange quotations, market prices, etc.) from the Internet. 12 per cent get this information from the press. While 10 per cent rely on their business partners and colleagues, and the remaining obtain tips from television and radio. 62 per cent of the respondents said this information help them respond quickly to the changing market

situation and better conduct financial operations and marketing studies. Statistic shows that the average age in Uzbekistan is 24 years of age. With a country of more than 24 million inhabitants and prevailing youthfulness of the current generation, the Internet potential is enormous.

Currently 39 companies in Uzbekistan have been granted licenses for provision of data transmission services, of which 19 are commercial, 15 providers work in Tashkent and the rest cover the surrounding regions. The major ones include: UZPAK, Naytov, Uznet, Eastlink (currently updating its license) CCC, Globalnet, BCC, Ishonch, and Simus. Local ISPs provide the following range of services: dial-up, leased-line connections, e-mail, DNS service, and web-design. One of the new trends in development of Internet services is radio Ethernet (RE) technology. RE technology brings a better quality solution for its clients. In partnership with US-based Winscom Technologies, Sarkor telecom has been successful in introducing radio Ethernet throughout the capitol.

Lacking financial reserves for investment in security systems, most local companies rely on Microsoft proxy servers as the only means of protection of their networks. Some of domestic firms explain this phenomena by the fact that the purchase price and installation of Internet security hardware exceeds the cost of the potential loss of company's information in the network.

Besides Microsoft proxy servers the other widely used security systems are: LINUX based BSDs or UNIX applications. These systems are prevalent even among the domestic ISPs. Most of them are obliged to use UZPAK, National Internet and data transmission clearinghouse, and channels to gain their data connection. Subsequently ISPs rely on UZPAK security tools to address their security concerns. The other Internet Service sub-providers, who use Naytov, the country's only independent ISP's network, rely on the security system it maintains. UZPAK and Naytov predominately use CISCO and Sun Microsystems network security products.

According to local experts, the Central Bank (CB) of the Republic of Uzbekistan owns one of the most advanced Intranet in the country. CB has a high quality network security system, with CISCO hardware and software. CB's extensive Intranet covers most of the regional centers in Uzbekistan. However, it would be premature to say that CB uses Internet Security tools, as there are no e-transactions in Uzbekistan.

In addition to CB, the National Bank of Uzbekistan, the Tax Committee, the Customs Committee, a variety of GOU Ministries and large enterprises, such as Navoi Mining Factory, and Almalyk Mining Factory, have sound corporate networks.

Large international corporations and company representative offices, diplomatic entities and some non-governmental organizations are among the few establishments, which invest in Internet security systems. Coca-Cola, Uzbek British American Tobacco, and Zaravshan Newmont Mining Factory maintain their own Intranets. Most of the Embassies located in Tashkent use some sort of Internet security hardware to protect their networks. For obvious reason, these companies are not willing to divulge any detail information. However, the most popular are CISCO, Sun Microsystems, Siemens, and NEC products.

According to informed sources, system administrators of the most domestic companies, which are showcased in the Uzbek web prefer installation of complimentary security operation systems, distributed under GNU and under BSD/Berkley license as well as free web-servers, such as various versions of Apache servers. Most of these systems function with Apache web-servers. Basically this is due to the compatibility of the system based on apache web-servers interact and integrate easily with FreeBSD and LINUX operational systems.

The selection of a choice of operational system usually depends on its vulnerability. Reviewing most popular operational systems in the local market, we can make the following conclusion – LINUX and Windows share the major stake of the market, up to 70 per cent. The rest are divided among Solaris, NetBSD and FreeBSD.

-Authentication, authorization, and administration (sometimes referred to as the 3As)
The standard authorization protocol for the majority of Uzbek enterprises use a standard scheme of password and logins.

Firewalls execute authentication-using IP-addresses, which are given to each server client and network device and can be replaced. Identification is a series of methods that allow the system to identify a user. Currently, the Password identification is the most popular and widely used method, however it is a common occurrence to have users create easy-to-guess passwords, which inherently do not provide a high level of security. There is a modest growth of enterprises that install access cards and smart cards systems.

-Firewalls

Firewalls provide a higher degree of protection in comparison with proxy applications. As we know, most of firewalls were created for UNIX systems, however lately several new products appeared in the market, namely Checkpoint, Raptor, and Seattle Software Labs Trusted Information systems products based on Windows NT platform.

According to a recent survey conducted by local analysts, the favorite firewalls among Uzbek companies are as follows: Step One and Watch Guard or Microsoft based applications. The other options include LINUX based FreeBSDs and Raptor. Generally, most of ISPs and large banks and enterprises use proxy servers and do not invest in expensive security systems, their reasoning being there is no necessity in having expensive security systems for the current level of existing information.

Hardware security systems, e.g. CISCO security systems exist in the market at a minimum cost of up to USD 5,000-6,000, which is not affordable to many local companies. The majority of domestic companies still use inexpensive security solutions.

-Virtual private networks

Virtual private networks (VPN) use advanced encryption and tunneling to permit organizations to establish secure, end-to-end, private network connections over third-

party networks, such as the Internet or extranets. Benefits of VPN include: cost savings, security, scalability, and compatibility with broadband technology.

By leveraging third party networks, with VPN, organizations no longer have to use expensive leased or frame relay lines and are able to connect remote users to their corporate networks via a local ISP instead of via expensive long distance calls to resource-consuming modem banks.

VPNs provides the highest level of security using advanced encryption and authentication protocols, which protect data from unauthorized access. VPNs allow corporations to utilize remote access infrastructure within ISPs. As such, corporations are able to add virtually unlimited amount of capacity without adding significant infrastructure.

There are a number of VPNs created by the large international corporations and local banks located throughout Uzbekistan. Coca-Cola - Uzbekistan, Uzbek British American Tobacco, Newmont Mining, National Bank, Uzbek Airways and Central Bank of the Republic of Uzbekistan utilize its existing infrastructure developing extensive VPN projects stretching from Tashkent to other regional centers and the outside world.

-Public Key Infrastructure, PKI

Currently PKI is one of the most popular terms in the sphere of protection of corporate networks. The PKI importance for corporate networks is growing worldwide. Overall use of PKIs becomes critical in protection of e-commerce and VPN. However, PKI did not reach the appropriate level of popularity among the corporate users due to low technological knowledge base of its components and architecture, complexity and high solution cost.

- Encryption

Uzbekistan does not have its National Algorithm and is working on its creation. So far Uzbekistan uses the Russian FAPSI agency's 64 KBs key. In general, encryption is mainly used by the local banks for securing transactions. All information pertaining to the use of encryption is still kept secret. It is only known that the Uzbek security agencies and force ministries hold strict control over encryption issues.

-Smart cards

There have been several attempts to create smart card payment systems in Uzbekistan, most recently by BGS Asia, an Uzbek-Austrian joint venture. BGS Asia is an exclusive representative of BGS Smartcard Systems AG, an Austrian company, which enjoys the exclusive rights for the direct universal transaction system (D.U.E.T.) technology. The company has successfully implemented this technology at the National Bank of Uzbekistan, Asaka bank, Pakhta bank and People's Bank of Uzbekistan. BGS Asia delivered approximately 70,000 cards, about 700 point-of-sale terminals and more than 50 ATM to banks. BGS Asia completed this project by creating the Interbank emission center for smart cards in D.U.E.T. standard and the processing center for Uzbekistan Banking Association. This center will unify the smart-card systems for the National Bank of Uzbekistan, Asaka Bank, People's Bank of Uzbekistan, and Pakhta Bank. Further, it will enable all other banks and future banks to join a common smart-card payment system in Uzbekistan.

There is an on-going project between Eurasia Technology Group and BGS Asia to design a more comprehensive e-commerce solution, which will utilize smart cards in Uzbekistan.

-Content screening, Anti-virus and Mobile code
Most of Uzbek companies use AVP created by Kaspersky laboratory. Norton Anti-virus and Dr. Web are among the other widely used programs. The Kaspersky laboratory has a significant presence in the CIS market.

-Data warehousing and information
Due to its adolescent stage of development of Internet in the country, Data warehousing is yet non-existent in Uzbekistan.

-Enterprise security
As noted by network solutions companies supplying security systems to local banks and enterprises, the number of enterprises, which realize the necessity of installing security solutions in, their growing networks are gradually increasing. It has become standard operating procedure to include a security upgrade for any new network solution project.

**31.3 Major trends**
Within the past two years Uzbekistan has experienced a sharp increase in the overall expansion of Internet service providers' (ISP) and users base. Since 1999, the growth of ISP totaled 300 per cent. The numbers of local users have increased to almost 80,000 countrywide. There is a dramatic upsurge of Internet related ventures, including Internet cafes and web-shops.

The Government of Uzbekistan (GOU) moves forward in an effort to privatize Uzbektelecom, its national telecom operator, in an attempt to increase Western investments to the country's growing telecommunication sector. Uzbek Agency for Post and Telecommunications (UAPT) plans to sell up to 51 per cent of its shares to a strategic investor, offering the rest to interested buyers in return for telecommunication equipment supplies. The government's plan is designed to have 70 percent of the company privatized ultimately. German Commerzbank AG was appointed as a financial advisor, to determine the amount of shares to be allocated.

According to UAPT official sources, Uzbektelecom may soon receive the exclusive rights to manage international telecommunications. This agency intends to issue an operating license to a company by the end of this year. This activity is yet another effort to attract more foreign investors. UzIntal, one of Uzbektelecom's newest divisions will allegedly be issuing licenses for Internet activities.

February 2001, GOU has confirmed and announced the feasibility study for the project of modernization and development of national data transmission network. The project is to be carried out in three stages within a five-year period. During the first stage, a central switchboard will be set up in Tashkent, the capitol, and link the national network to international and local information networks, including the Internet. This switchboard will operate the network and ensure information protection. The second and third stages include the installation of regional

switchboards, which will shape a single inter-regional network. It is estimated that the project will support a 20-fold increase in the volume of information transmission services in the country, with the number of users growing by approximately 11.8 times. The project's preliminary estimated cost is USD 10-15 million. US Belam Inc. is the winner of the tender for the first stage of this project, and has signed a contract worth USD 5,184 million with the joint stock company Uzimpexaloka.

The second stage of this project is dedicated to the modernization of telecommunications in the areas surrounding the Aral Sea. This tender is tentatively scheduled for April of this year. The objective of the Japanese funded tender is the modernization of the telecommunications infrastructure of the Karakalpakstan Autonomous Republic, Navoi, Bukhara and Khorezm regions. Japanese OECF Fund started the fund in 1996 with the selected winner in 1997 of Mitsui/NEC. Lately Overseas Economic Cooperation Fund was transformed into Japan Bank for International Cooperation (JBIC) and continues its activities in Uzbekistan.

The new JBIC loan to GOU will cover phase II of the current project and lasts for 30 years with an interest rate of 3 per cent, which is equivalent to Japanese yen 12,692 million or approximately USD 106 million.

The upcoming tender will cover the following items:

1. Switching equipment for 265,000 channels
2. WLL systems for 10,000 subscribers
3. Optical networking systems including fiber and SDH mixes
4. Network management systems
5. Radio and television broadcasting

Abl-soft Company and Uzbek Chamber of Commerce along with entrepreneurs initiated one of the most interesting projects dedicated to the development of domestic usage of e-commerce. The two main partners will develop a new multi functional information center – Maroqand. Maroqand will connect 12 regional centers. The main idea of the center is to fill the gap of e-commerce literacy among the small and medium size businesses and create the comprehensive database of companies, which will interact with each other through the Maroqand data network. For a relatively low monthly membership fee of UZS 6,000 – 7,000, local businesses throughout the country will be able to advertise their products or services at the site. Specially designed software will allow the search and selection of all members. Each member will have his/her own e-mail address. While Alt_soft will develop the technical base, the Chamber will assist in the distribution of the initiative through its branches. The founders of the project explained that they want to assist local businesses to get a taste of e-commerce at no risk.

**- Market obstacles**

There are several factors which hinder Internet development in Uzbekistan, including:

- The geographical remoteness of existing high-speed and high-capacity Internet backbones that make the Internet service a more expensive venue for the domestic end-users;

- Lack of general knowledge and sufficient experience among computer users with Internet-analogous systems;
- Absence of a countrywide electronic infrastructure network necessary for the initial Internet development.
- Uzbekistan's state and regional networks predominately have vertical Internet connections, which makes it difficult to embrace the whole country by the unified network;
- Lack of legislative base for constructing both local and worldwide information networks;

The following reasons restrain the development of the Internet Security market, including:

- High level of software piracy
- Absence of the sufficient information on the Internet
- Low financial capacity
- Hard currency convertibility issue

**- Key players in the Local market**

UZPAK

UZPAK is a National Data Provider. UZPAK network corresponds to the requirements of Consultative Committee on International Telephony and Telegraph. UZPAK has a "ñ" class network and domain: "UZPAK.uz". UZPAK is connected to a high-speed channel of 384 kbit/s through Seabone ISP, with the capacity of expansion to 1 mbit/s.

UZPAK provides 24-hour service in Tashkent and to all regional centers. UZPAK is working on the base of Nortel-Telecom equipment. It uses ITI protocols (x.3/x.28/x.29) .x.25, x.75, frame relay and SNA. UZPAK implements secure intranet networks for the state and private enterprises. UZPAK provide leased and dialup connections. UZPAK has intranet connection with Turpak and Sovam networks.

**Naytov**

Naytov Co. was established in 1994 and is one of the leading computer companies engaged in: computer distribution, system integration, LAN – WAN development and internet services. The Company has its branches throughout the Republic. Naytov operates a partnership with Sovam Teleport, one of the largest Russian telecommunication service providers. Naytov provides ATM, frame relay and x.25 services. The company also provides leased lines for fast and quality Internet connection. It is the second largest ISP in Uzbekistan.

The Tashkent City Telephone Station (TCTS) dominates among the companies providing fixed line services. Taking advantage of having its own digital network throughout the city and proximity to Trans-Asian fiber optics network, TCTS has been developing a new range of the fixed line communications. In 1999 after TCTS has launched an extensive market campaign offering somewhat low prices for ISDN and video-conferencing, these services have quickly found its customers among the local banks, foreign representative offices and diplomatic missions, hotels and even private users.

Tashkent City Telephone Station (TCTS) has recently become an ISP. TCTS owns the largest telephone network in the capitol and plans to utilize its existing clientele to develop more value-added telecom services.

Eurasia Technology Group LLC. On September 6, aiming to systematize the existing Uzbek and other CIS web sites into comprehensive portal, which would combine all current domestic resources into one site, Eurasia Technology Group LLC (USA) has launched a unique information portal - Esezam.

Esezam Internet portal has united 9 Eurasian countries: Armenia, Azerbaijan, Georgia, Kazakhstan, Kirgizstan, Russia, Tajikistan, Turkmenistan and Uzbekistan into a unified information space for the first time. The portal includes the following information services

Portal creates satellite-projects, information sites and vertical portals, aimed to fill the information vacuum of Central Asian and Caucasian region. Teams of professionals from the United States, France, Russia, Israel, Uzbekistan, Kazakhstan, Georgia, Kirgizstan, and the Ukraine are working on this portal. Esezam specialists are engaged in a new e-commerce initiative that will cover Uzbekistan.

**Legal framework**

The State Committee for Science and Technology (SCST) has outlined the development of informatization sphere in Uzbekistan as follows. In 1992, SCST was the first agency to address the issue of the importance of developing information technologies for the Newly Independent Republic. This has resulted in an issuance by the Cabinet of Ministers resolution - On Informatization - in 1993. In 1994 SCST drafted a unified concept on computerization of the Republic of Uzbekistan emphasizing the following purposes:

- Development of a country wide information zone;
- Development of sound banking information system;
- Computerization of social services sector
- Science and technical computerization;
- Development of the program and software industry.

Congruently, in cooperation with GOU SCST identified the concept for creating the national data transmission and Internet nodes. In 1995 this agency assisted in preparation of a Cabinet Ministers Resolution on copyrights, which addressed the protection of software and application programs from piracy.

The new telecommunications law adopted in 1999, outlining three resolutions on the UZPAK activities has clearly shown the GOU understands the necessity in the development and modernization of the existing telecommunication infrastructure. Following February 5, 1999 resolution, UZPAK became the state enterprise on exploitation of the national data transmission network.

Uzbekistan has chosen a so-called Chinese method of the Internet development with severe restriction on political and opposition web-activities. After the creation of UZPAK, the major Internet clearinghouse and data network provider, in 1999 all ISPs had to be re-registered with UZPAK and obtain new ISP licenses. Since this

procedure ISPs can now only provide services through UZPAK lines. Only Naytov, a U.S. company, is a de-facto independent ISP operating in Uzbekistan.

UZPAK regulates of the Uzbekistan territory. However, with a dramatic growth of the local Internet network, UZPAK simply does not have sufficient capacity to control the spread in popularity of the World Wide Web. Many ISPs use a two-channel method and manage to send information through UZPAK provided channel, but use their own dish for uploading information. Thus circumventing the control mechanism of UZPAK. There have been several reports in the western press about the strong GOU censorship over the local web-net. While admitting the serious infringement of basic rights for the freedom of expression and the right for privacy, we would like to emphasize that according to the opinions of local computer experts, UZPAK can not control all Uzbek web-sites with the existing equipment capacity. UZPAK uses filtration and tend to censor e-mail, there are cases where Internet users were chased and warned for accessing certain prohibited web sites, namely Islamic fundamentalist and terrorist sites, Uzbek opposition sites. The UZPAK official standpoint is that every country has the right to protect its national security interests. On the other hand, there have been cases where UZPAK could not trace the network intruders, which used its clients accounts. Currently, UZPAK has had several problems: lack of professional personnel, insufficient telecommunication equipment base and lack of transmitting capacity.

On April 23, 1999, the Cabinet of Ministers approved a program for the modernization and development of a national data transmission network over the next five years (1999 – 2003). This program is slated to conduct technical measurement for expansion of data transmission network in Tashkent, Nukus and other regional centers in 1999-2001 in the first wave; and in the district centers in 2000-2003 in the second wave. It also provides the base for increasing of a network bandwidth and installation of a high speed network technologies such as ATM and frame relay.

Apart from CIS countries, only Russia seriously attempted to address the growing need for creation the necessary legislative tools for increasingly developing e-commerce. Uzbekistan does not have any laws and regulations covering e-commerce development.

### 31.4. Competitive analysis

Finding reliable domestic distributors, along with competitive pricing and credit terms provide a good package for entering market of information technologies.
U.S. Commercial Service is actively assisting U.S. companies seeking distributorships, and offers a number of business counseling and trade facilitation programs.

European and Asian companies such as: Siemens, NEC, and Huawei are the main U.S. competitors in the Internet security and network solutions equipment marketplace.

Domestic vs. third country key-players

Statistics show that by year's end the number of subscribers of the Internet services in Uzbekistan will have at least a 5 per cent increase. However, the existing number of subscribers lags far behind average indicators worldwide. Throughout Central Asia, Uzbekistan comes second in terms of the number of users, after Kazakhstan. The majority of Internet services subscribers are Tashkent residents, with the rest located in Samarkand, Bukhara, Ferghana and other regional centers. For the majority of the country's population, Internet services are still prohibitively expensive.

90 per cent of ISPs are located in Tashkent. There is a handful of ISPs providing Internet services throughout the regions. Companies, which provide Internet services are also the largest consumers of these services, including Internet access, web design, and banner advertisement). International corporations and representative offices, large industrial enterprises are second-position in terms of utilizing Internet related services. Private businesses and private users comprise the third tier of the Internet services market. The range of Internet services and prices varies widely. With 7 core ISPs and new-comers appearing rapidly the existing competition among cellular providers is becoming stiff which results in a gradual decrease of tariffs on Internet services, which in return, allows the number of potential customers to expand.

The majority of the Internet security equipment is imported from the United States. European and Asian products share the rest of the market. Domestic enterprises involved in manufacturing of telecommunications equipment do not produce Internet security hardware equipment.

Apart from United States, the rest of Internet security hardware equipment is imported from Japan, Germany,
Israel and China. These companies include NEC, Siemens, RAD, Huawei and others.

U.S. market position

U.S. market position is strong in the Uzbek market for Internet security equipment. CISCO is the comprehensive leader in the security hardware solutions. Microsoft solutions are widely utilized by most of the Uzbek users.

CISCO is a worldwide leader in e-economy and networking solutions. CISCO actively promotes the idea of e-strategy aiming to improve effectiveness and efficiency of businesses and government structures throughout the world.
Many people are familiar with the Internet and are aware of the importance of the net information. 85 per cent of the technological equipment for the Internet is produced by CISCO Systems.

Originally CISCO operated in the Uzbekistan market through its Moscow representative office and CISCO’s local distributors. However, this situation has recently been changed, this February CISCO held a major seminar covering various issues related to CISCO world-wide activities, its networking products and plans for the future expansion into the region. CISCO considers Uzbekistan as the major market in the Central Asia, and will establish its office in Tashkent shortly.

3com, Nortel Networks, Lucent Technologies, and Sun Microsystems equipment are also represented in the Uzbek market. Sun Microsystems hardware is widely used by local ISPs.

Global Tele systems group (GTS) is an American corporation, owner and operator of telecommunication services. GTS maintained its presence in the market CIS since 1989.

Golden Telecom is a holding group, which owns all company's actives throughout Russia and CIS.

Teleross was created after the merger of three network operators, Sovam Teleport, Teleross and TCM. Its total annual revenue comprises USD 90 million. Teleross provides data and Internet transmission in 90 Russian cities as well as in several CIS countries. Its trademark is Golden Telecom.

Golden Telecom, Inc., (listed in NASDAQ, ''GLDN') is a leading facilities-based provider of integrated telecommunications and Internet services in major population centers throughout Russia and other countries of the Commonwealth of Independent States (CIS). The company, one of the largest in Russia and CIS offers competitive local exchange carrier services using its overlay network in Moscow, Kiev and Saint Petersburg. The company manipulates data and long-distance services using a fiber optic and satellite-based network, including more than 120 combined access points in Russia and other countries of the CIS. It has dedicated and dial-up Internet Access to businesses and consumers and limited popular Internet content through several web brands, including its Russia-On-Line portal.

This company is one of the fastest growing in CIS and it is managing fast growth strategy by acquiring telecommunication companies in different CIS countries.
On October 2, 2000, Golden Telecom announced its plans to strengthen its mobile communications strategy in Russia and CIS by agreeing to acquire 18 to 24 percent of MCT Corp. (``MCT'') in exchange for GTI's Russian mobile operations. After this transaction is settled, MCT's properties will cover a population base of more than 100 million people, including the four largest cities in Russia, as well as Uzbekistan and Tajikistan. Global TeleSystems Group, Inc. (USA), major international telecom and ISP operator, holds approximately 63 percent of Golden Telecom's outstanding shares.

After acquiring of SDH channel with 2.4 GB from Moscow to Stockholm, Golden Telecom has become the first company that owns the largest international capacity in CIS countries and exceeds the total-channel capacity of all its competitors. The Company's network is connected with e-bone broadband network located throughout Europe, which provides traffic with a 2.5 GB/s speed.

Another Telecom Company, Globecomm Systems Inc. (GSI) along with its subsidiary Netsat express operates a new hybrid satellite terrestrial (HST) IP network with global coverage even more extensive than the SITA network. GSI designs, assembles and

installs ground segment system and network solutions complex and changing communication requirements of its customers.

Last year GSI discussed the possibility for the construction and installation of a satellite network for Uzbekistan Airways (HY) under a subcontract with Thomson-CSE. GSI intends to provide a complete analysis of the traffic characteristics and flight operations messaging among Worldspan, the Delta operations control center in Atlanta and HY headquarters in Tashkent. Based on that study, GSI plans to recommend an equipment upgrade for a high speed IP virtual private network including provisions for e-commerce transaction security firewalls and 24x7 network status monitoring.

Netsat express (NSE) is a GSI subsidiary, which provide a core satellite and enterprise communications solutions to bring Internet connectivity to emerging markets such as CIS countries. NSE currently has over 50 network service contracts with enterprises in emerging markets for access to its hybrid satellite/terrestrial high-speed IP global network.

Given the high potential of the Uzbekistan market for the Internet services and related networking equipment, hard currency convertibility and low purchasing power factor place significant barriers to an active U.S. investment campaign to the country. U.S. companies operating in Uzbekistan must be cautious in their approach in future investments. Several U.S. companies have already faced severe problems in retaining their profits and further re-investments. The country's worsening economic situation, the lack of transparency in the regulatory system, involvement of state institutions in commerce and numerous red-tape problems hamper the process of real development within this sector.

Best sales prospects for the U.S. companies providing the Internet security related equipment include the following:

A) Internet Service Provision

The largest consumers of Internet services are the local ISPs. Generally a medium or large ISP would own CISCO or Sun Microsystems hardware for protection its network. Security-wise the smaller sub-providers depend largely on their ISPs. Currently, there are two major ISPs, Naytov and UZPAK, that own the largest share of the Internet services market. However, the number of ISPs is gradually increasing, with new players competing in the Internet Access Provision market.

B) Banking sector

Expansion of LAN, VPN and preparedness for the e-commerce activities reveals large local banks as a good opportunity for U.S. investment in networking systems, hardware and software solutions.

C) International Corporations located in Uzbekistan

D) Domestic industrial enterprises, GOU agencies and ministries

Statistical information

- Utilization and penetration of Internet

As noted above there are presently 39 ISPs in Uzbekistan. Below is the statistics of market penetration by ISPs compiled by local IT experts:

Internet and Data Transmission Companies

UZPAK - 45 per cent
Naytov - 40 per cent
Others - 15 per cent

There are more than 1,000 local web sites registered on the world web-network.

State and noncommercial organizations – 30 per cent
Commercial sites – 45 per cent
**Information sites – 10 per cent**
Entertainment or other sites – 15 per cent

According to Naytov.com, a company has an average 60 to 100 new dial-up users monthly. The majority of its users of the Internet services are Tashkent residents. There is a growing market for Internet services in the Fergana Valley, which is higher than in the other regions.

The major problems faced by domestic users are low connection speed and high tariff rates. As more and more regions within country and cities acquire new digital telephone equipment and fiber optics channels, the quality of Internet connection is expected gradually to improve.

The best example of the growth potential is the dramatic increase of Internet cafes in Uzbekistan. There are more than 20 Internet cafes in the city-center of Tashkent, with an estimate of an additional 40 establishments throughout the entire city. Besides Internet access, city web-cafes have many additional services, including computer games, copying services, and computer processing, much like the copy centers in the United States, i.e. Kinko's. With an entrance fee ranging from UZS 500 to 1,500, 50 per cent of cafes reports an average number of monthly users in the 400-600 users span. Many cafes owners tend to open Internet cafes in the center of the city or closer to universities and other educational centers, which helps them attract larger numbers of student customers.

Retrieval of Economic Information:

Internet - 71 per cent
Press - 12 per cent
Word of mouth - 10 per cent
Television and radio - 7 per cent

E-commerce

E-commerce in Uzbekistan should be viewed in the long-term perspectives. However, there are several major reasons preventing quick e-commerce development such as:

Lack of a legislative base
Lack of a credit card system
31.1.1 Local populations mistrust of the current banking system

Low Internet literacy

On an optimistic note, there are niche opportunities, which should not be underestimated. Recently local firms have developed several web-shop projects. The larger ones were created by Zeppelin ltd.(www.zeppelin.uz) and Lex-group (www.ippoex.com). Most of web-shops provide a structure of cash-and-carry system and specialize in fast food, flowers, electronics, and home appliances. According to the owner of Zeppelin.uz, he sees e-commerce as the next phase; so far the company wants to facilitate general information on e-world among the general population. The site had 4,533 visitors since it opened in November 10, 2000. The companies involved in e-solutions consider B2C as the first stage of development of this emerging market.

Regional opportunities

Market research reports: International Market Insights (IMI) are available on the National Trade Data Bank and BISNIS web-site for telecom industry in the Russian Federation, Ukraine, Kazakhstan, and Kirgizstan:

Overview of E-commerce Development in Russia (01/01)

Overview of Electronic Commerce (11/00)
E-Commerce Brief: Belarus (8/00)
E-Commerce Issues and Seminars in Russia (8/00)
Uzbekistan: Internet Service Market in Uzbekistan (6/00) Ukraine: Internet Service Providers Invest in E-Commerce (2/00)
Ukraine: List of Internet Services Providers (2/00) Kazakhstan: Credit Card Fraud on the Internet (1/00) Ukraine: ISP Global Ukraine Introduces Web Cards (1/00) Russia: Internet Broadcasting (11/99) The First Virtual Bookstore in Ukraine Gains in Popularity (11/99) Russia: Trade Publications on Internet Issues (1/99)

Companies wishing further information on this market sector can contact:
Ms.Tyrena Holley
Senior Commercial Officer
Mr. Andrey Gidaspov
Commercial assistant and telecom and IT sector specialist
Telephone: [998](71) 120-67-05 or 120-67-06
Fax: [998](71) 120-66-92 or 120-66-76
E-mail: Andrey.Gidaspov@mail.doc.gov

International mailing address:
41 Buyuk Turon Street, 3rd floor,
Tashkent 700000 Uzbekistan
U.S. mailing address:

U.S. Embassy Tashkent - Commercial Service,
Department of State
7110 Tashkent place
Washington, DC, 20521-7110